

FIG. 1

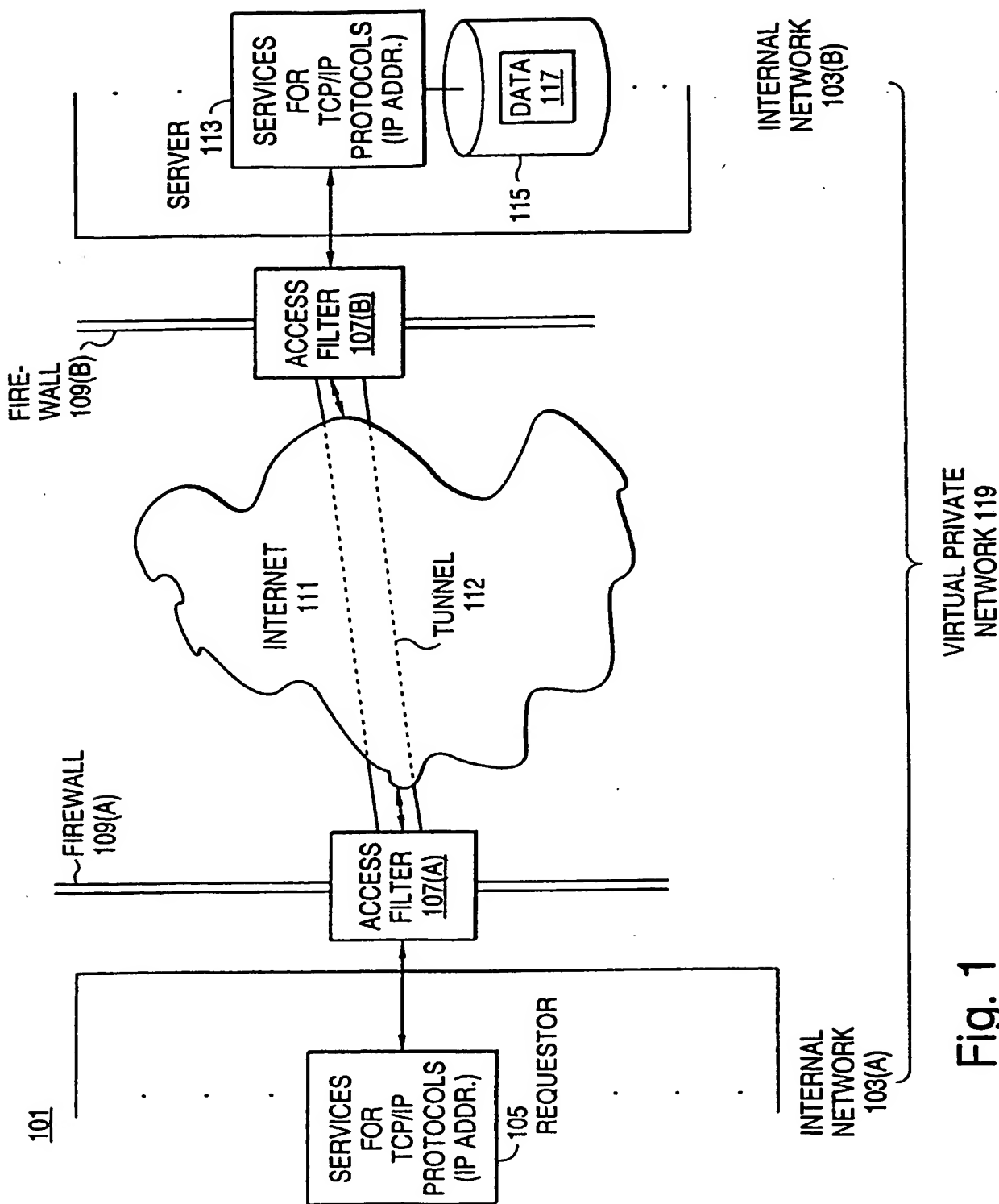


Fig. 1

FIG. 2

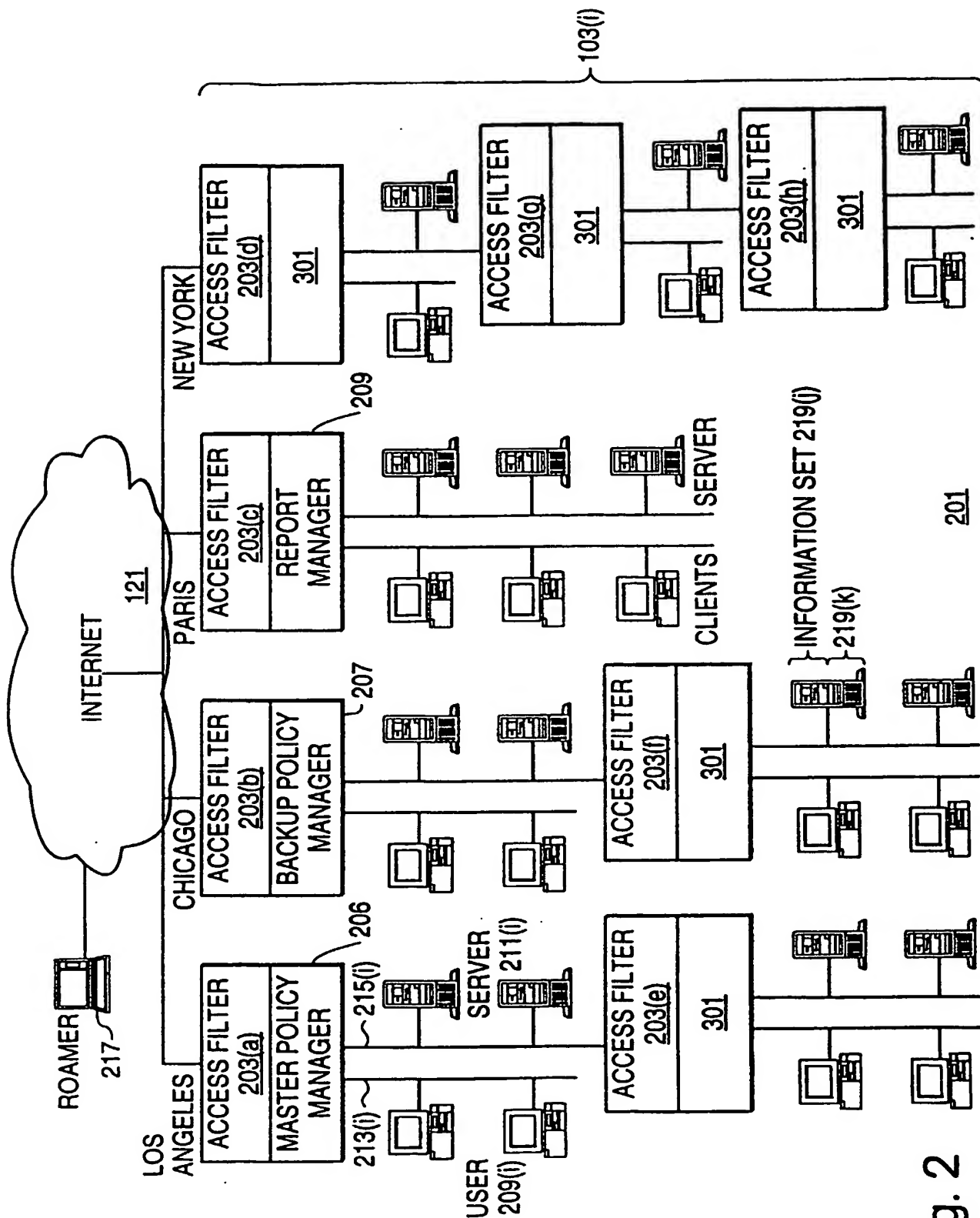


Fig. 2

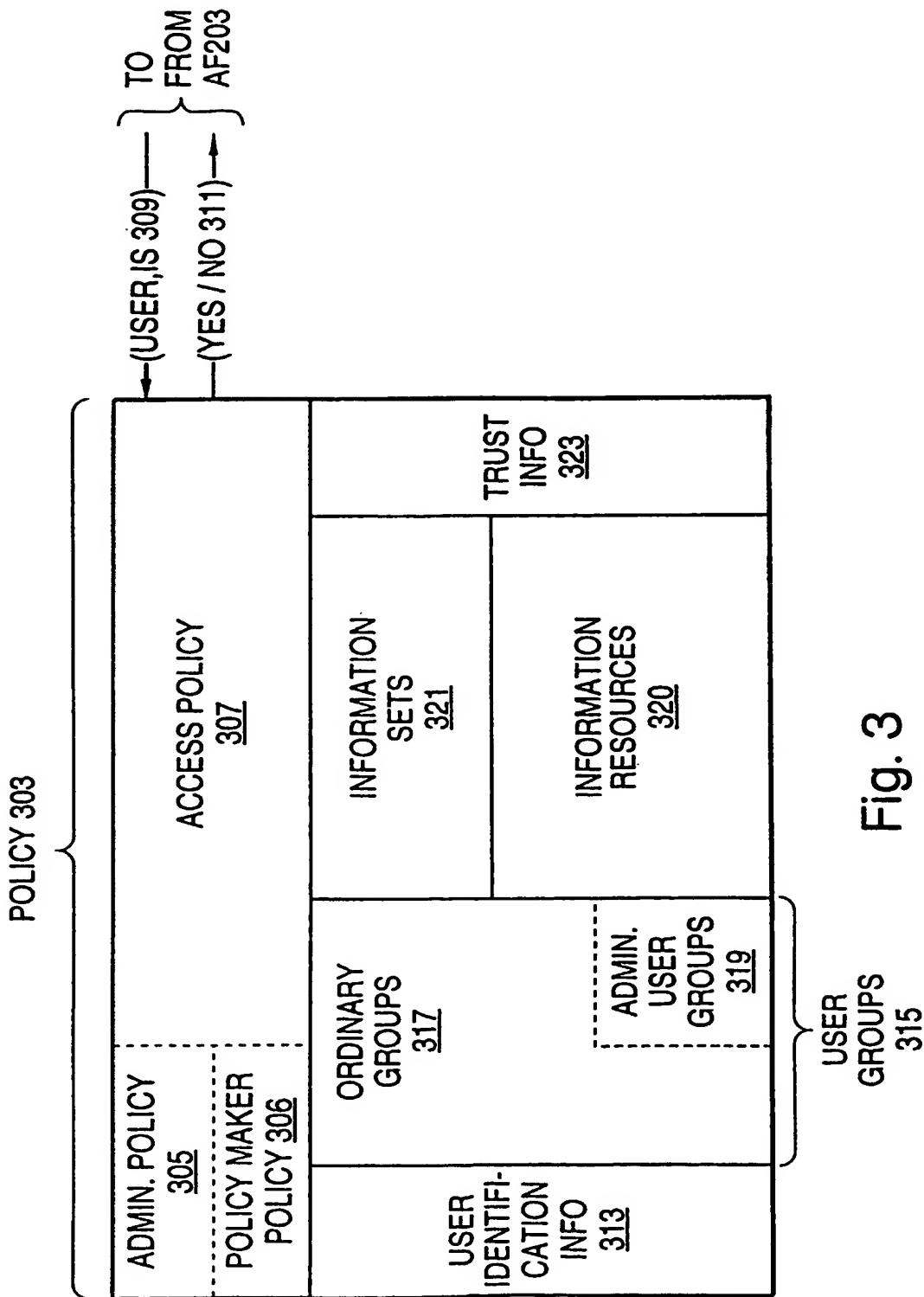


FIG. 4

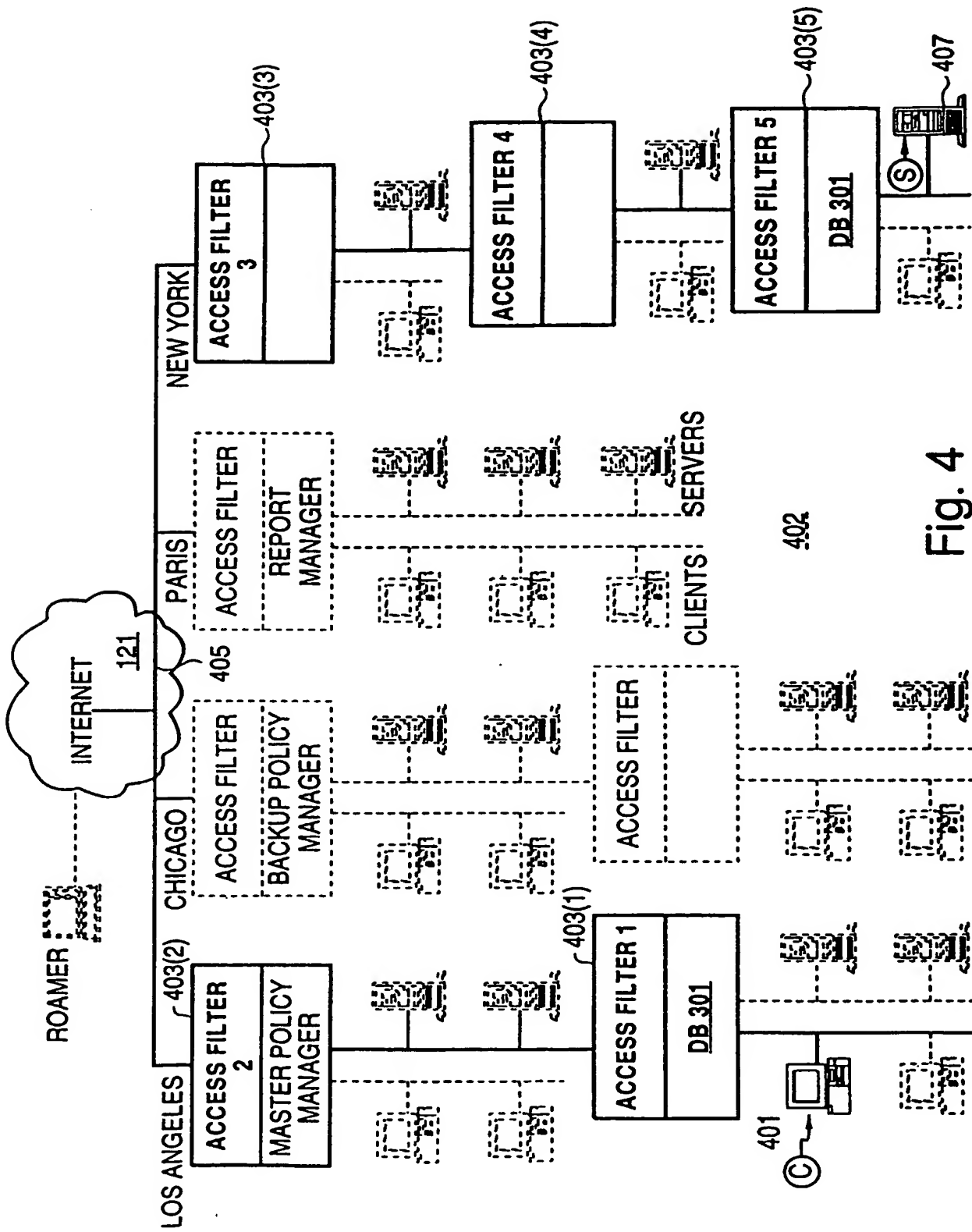


Fig. 4

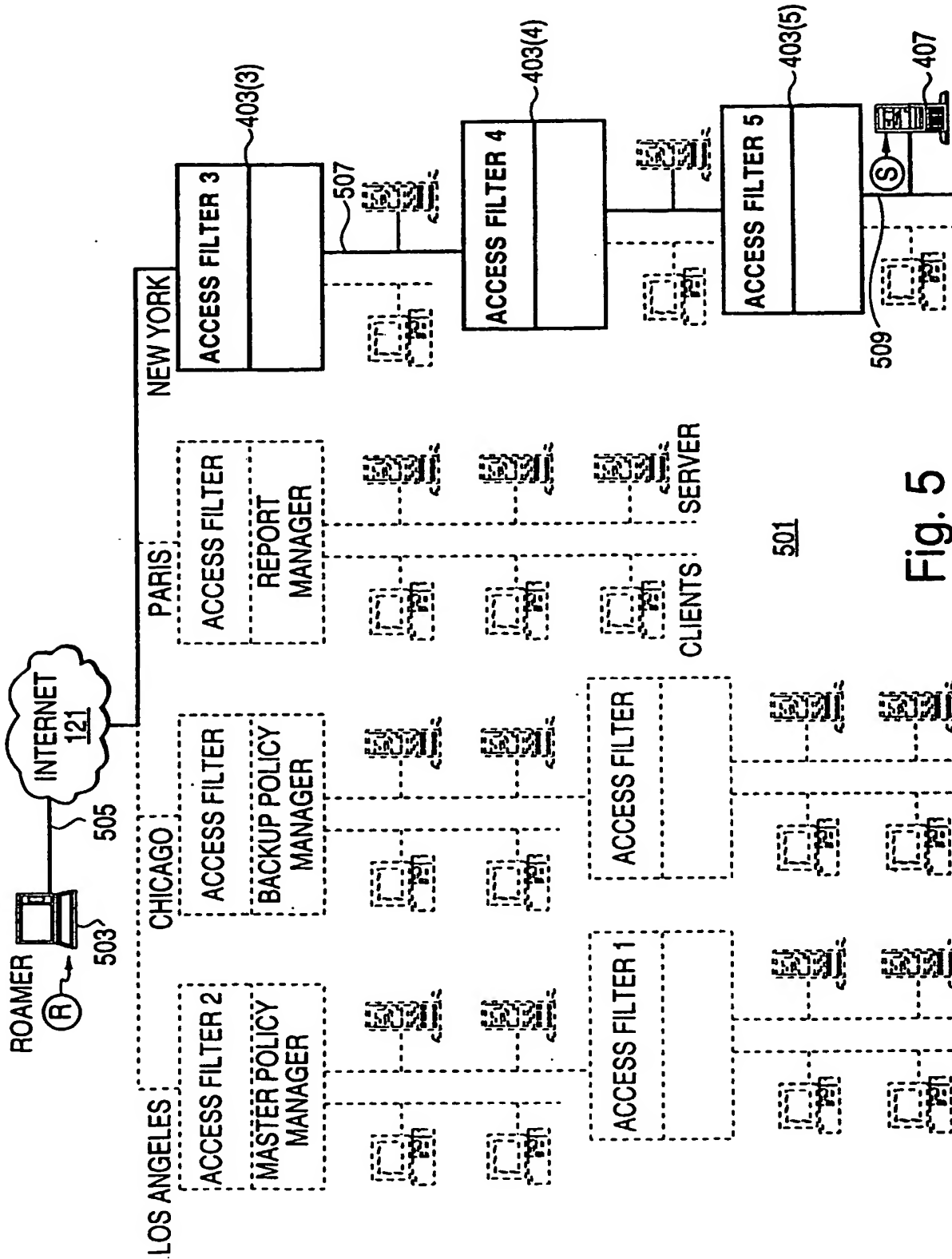


Fig. 5

Trust / Data Sensitivity Level	Minimum Encryption	Minimum Authentication
Top secret	3DES	Certificate via SKIP
Secret	DES	Certificate via SKIP
Private	RC4-40	Windows ID
Public	None	None

603 609 607

609(1) 609(2) 609(3) 609(4)

601

Fig. 6

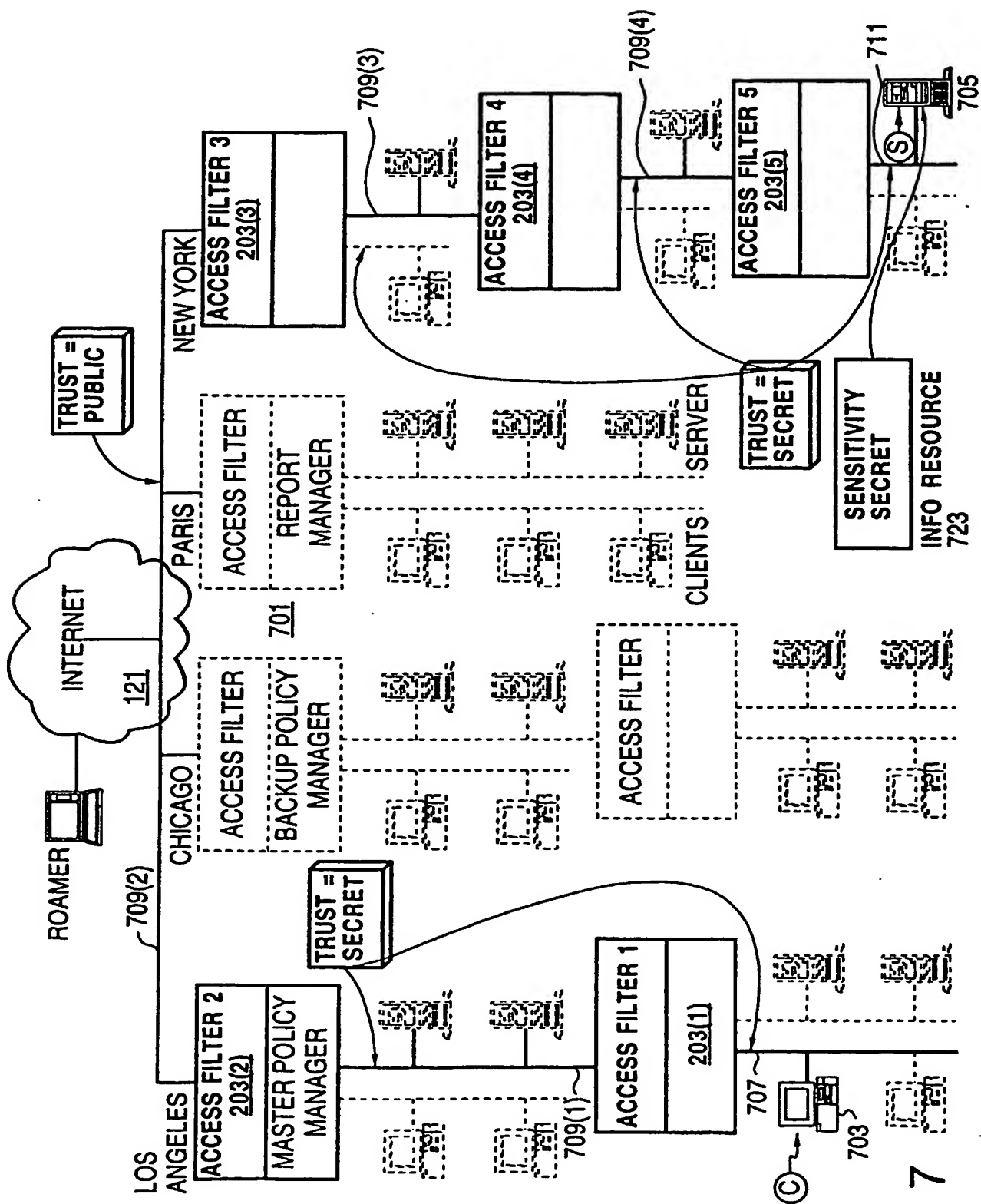


Fig. 7

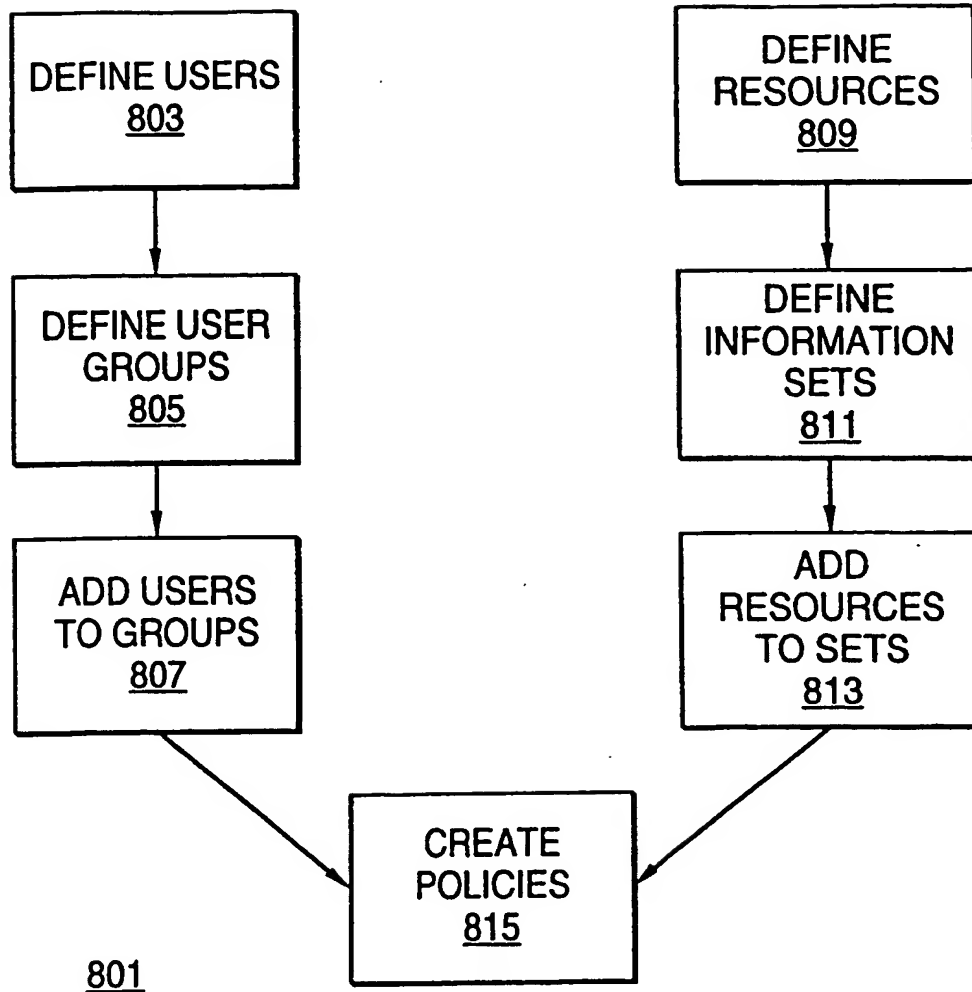


Fig. 8

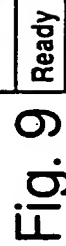


Fig. 9

1001

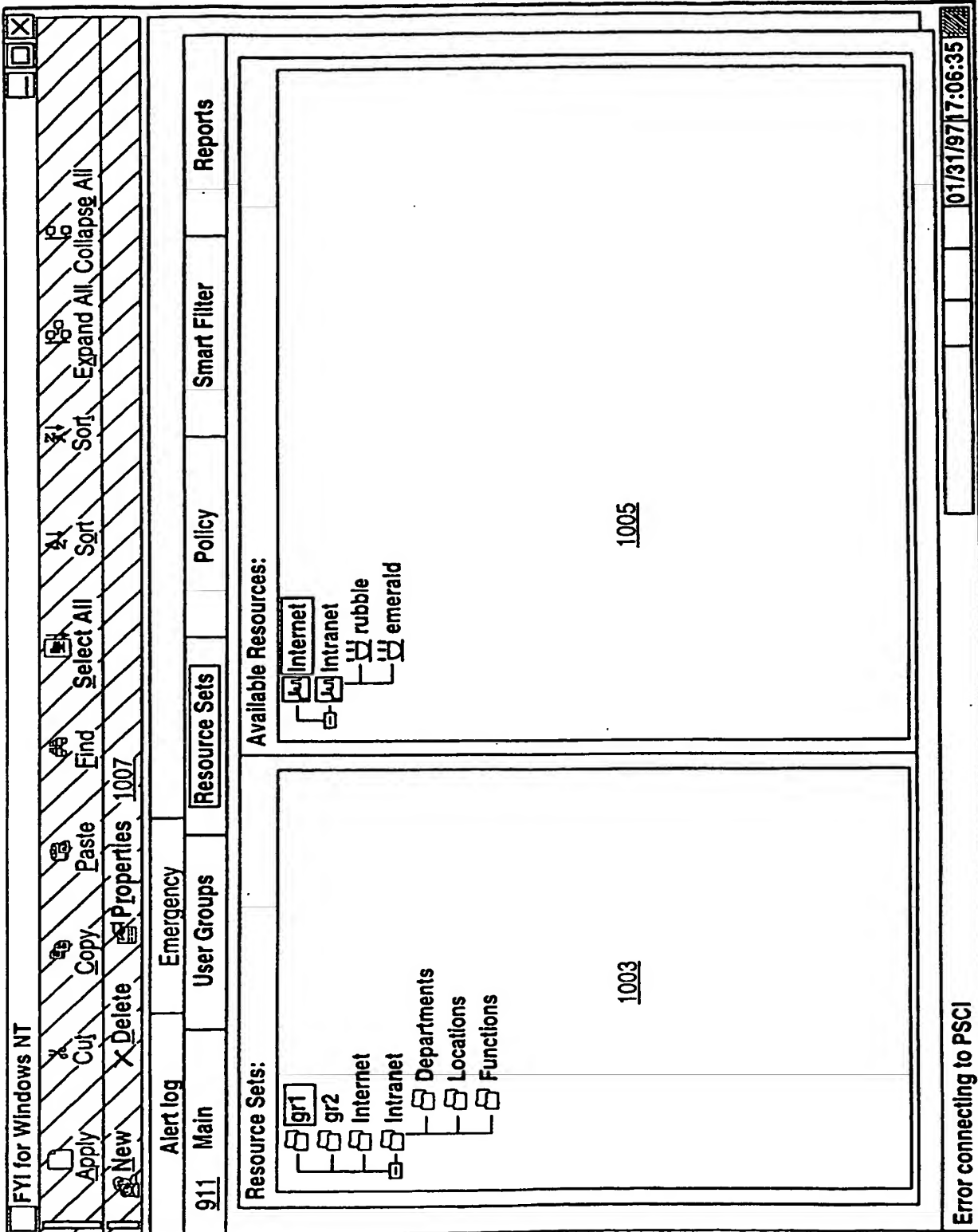
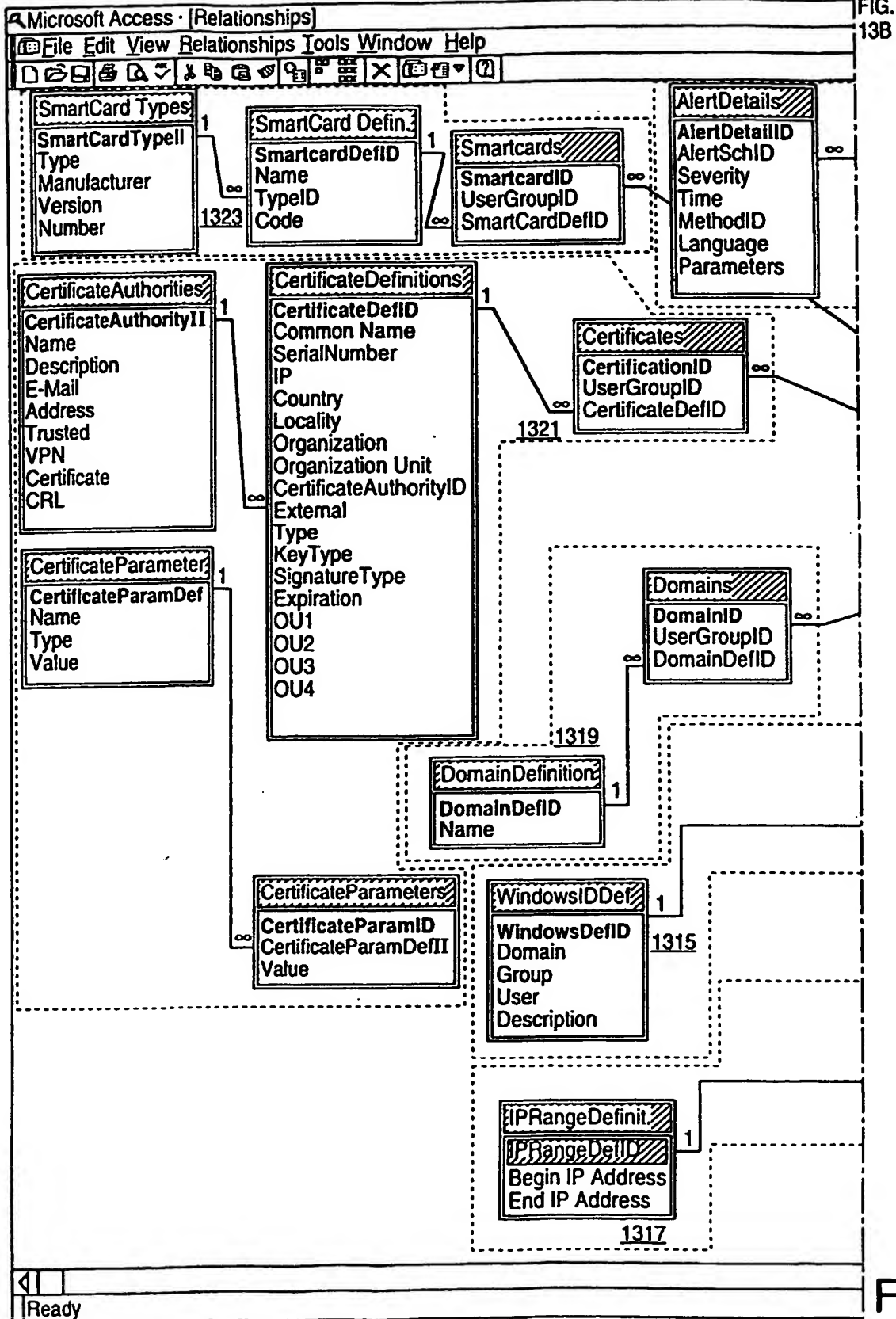


Fig. 10

Fig. 12

Fig. 12

1U/019101



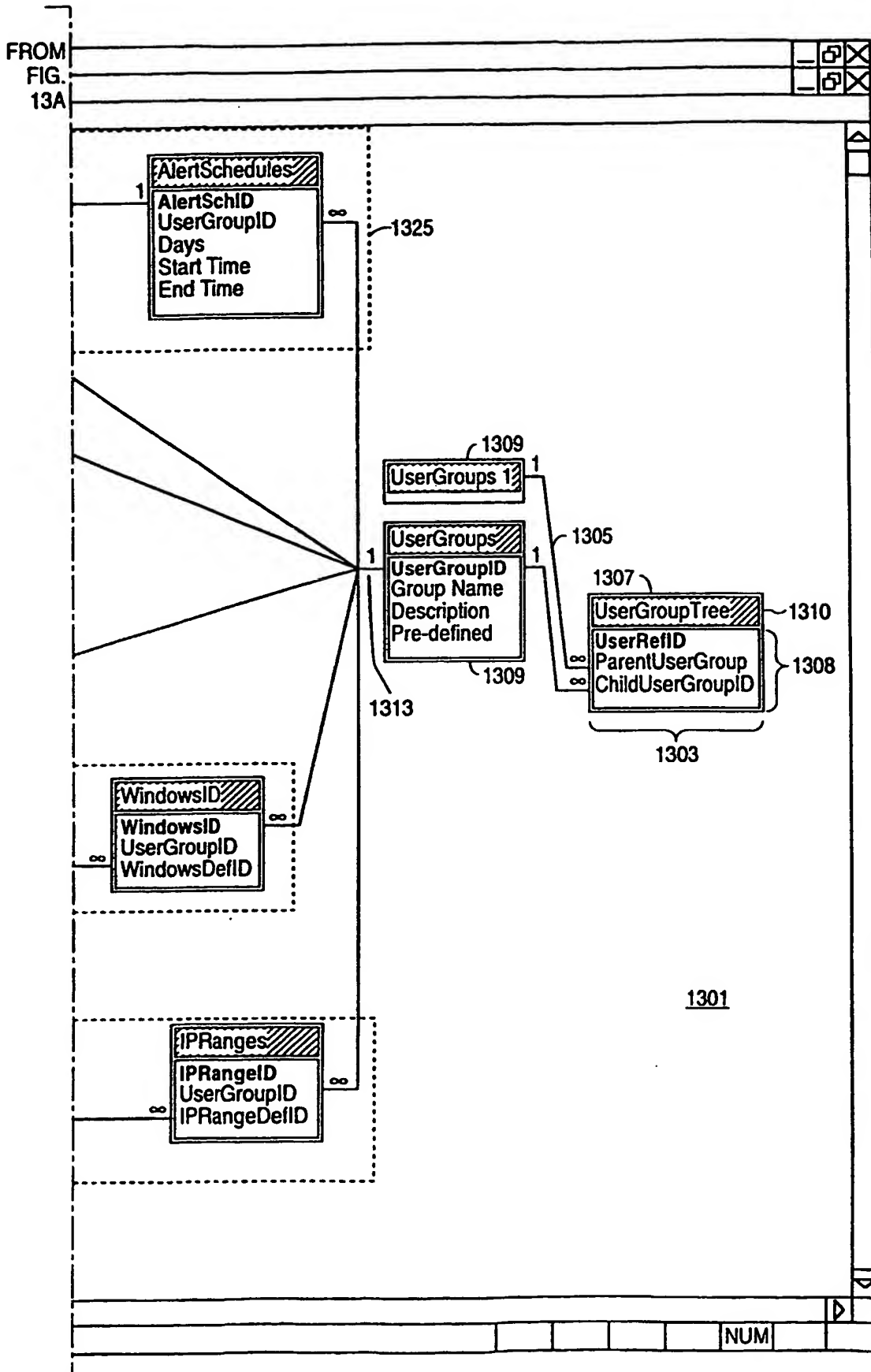


Fig. 13B

FIG. 14

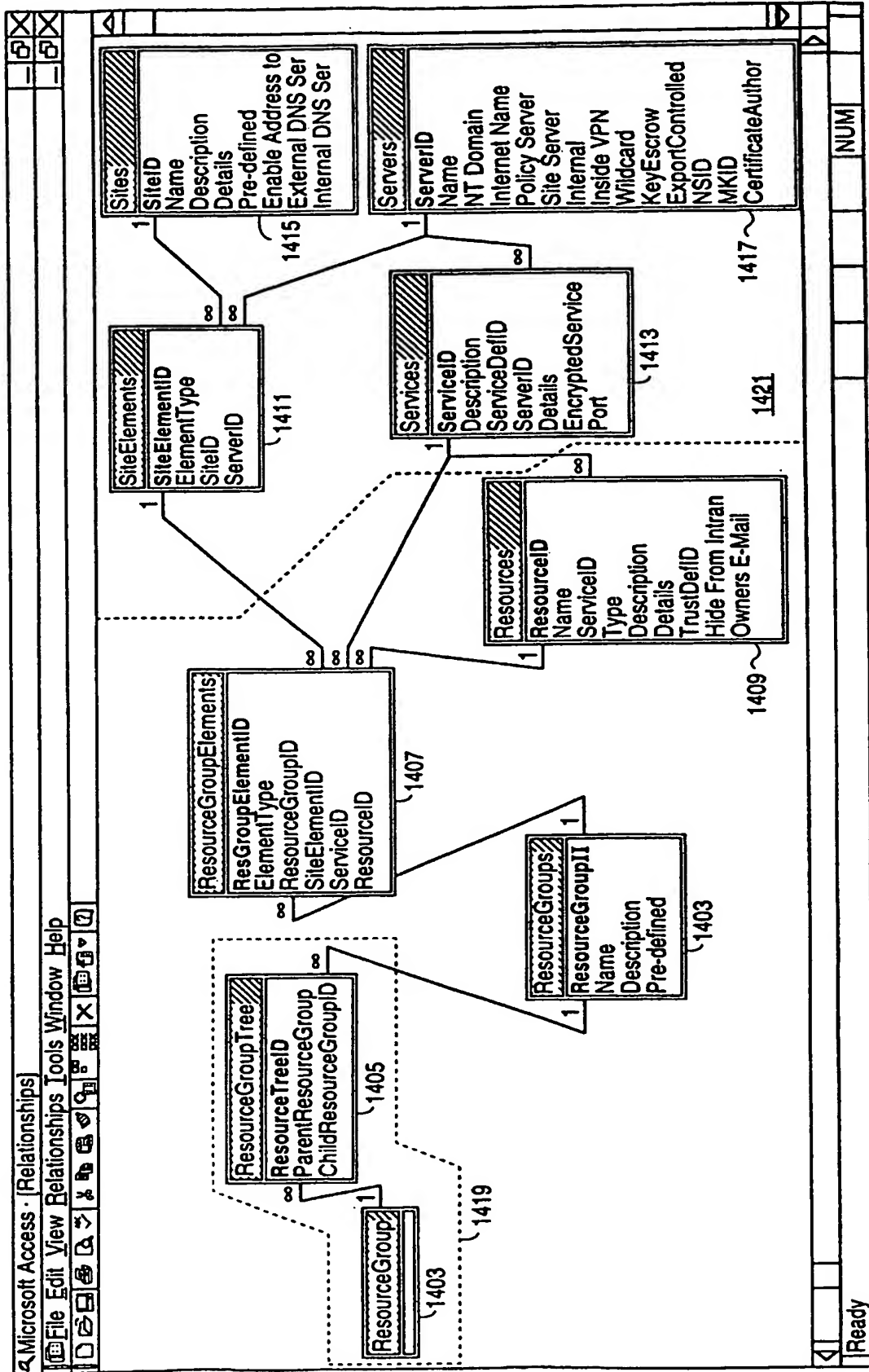


Fig. 14

FIG. 15

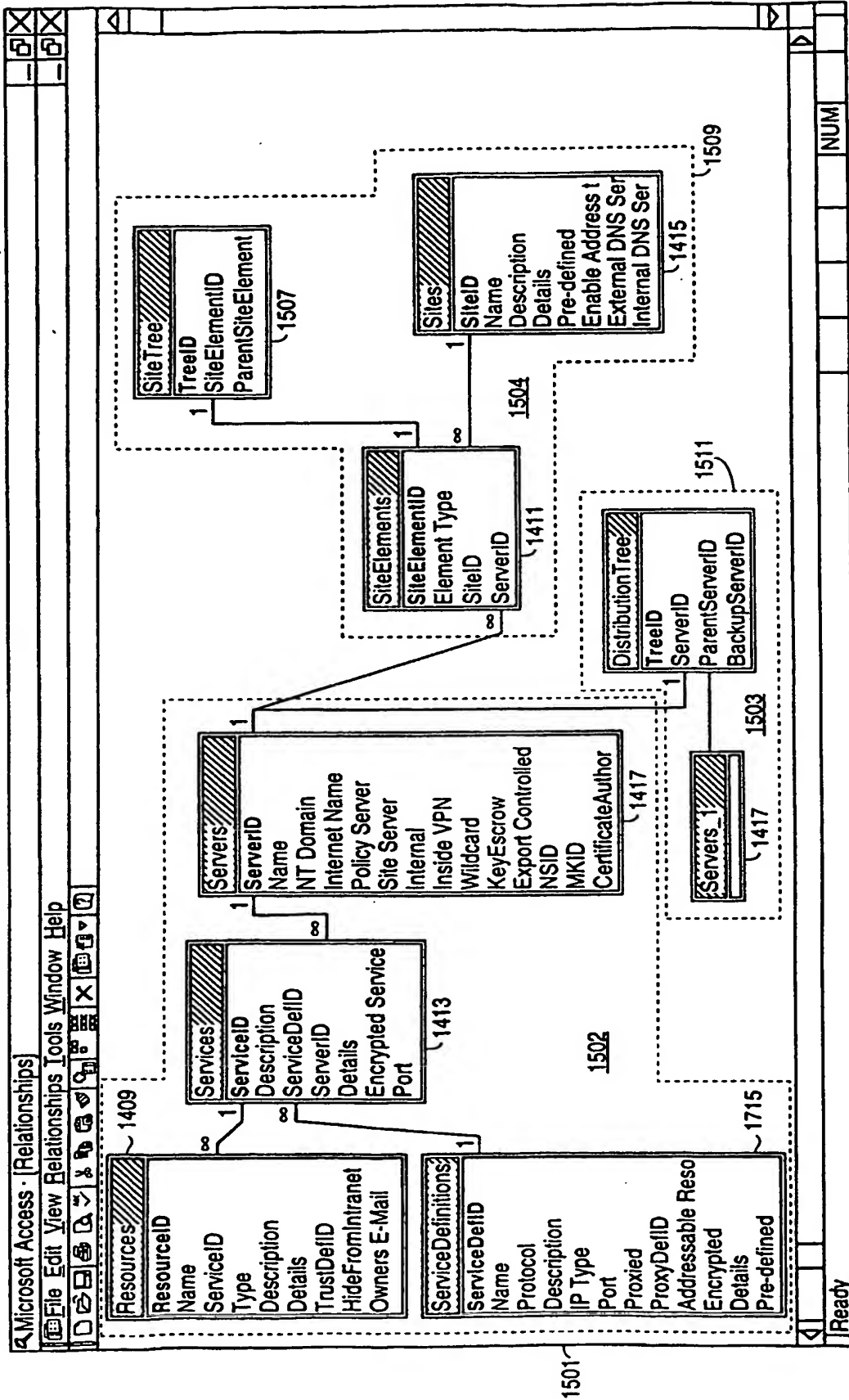
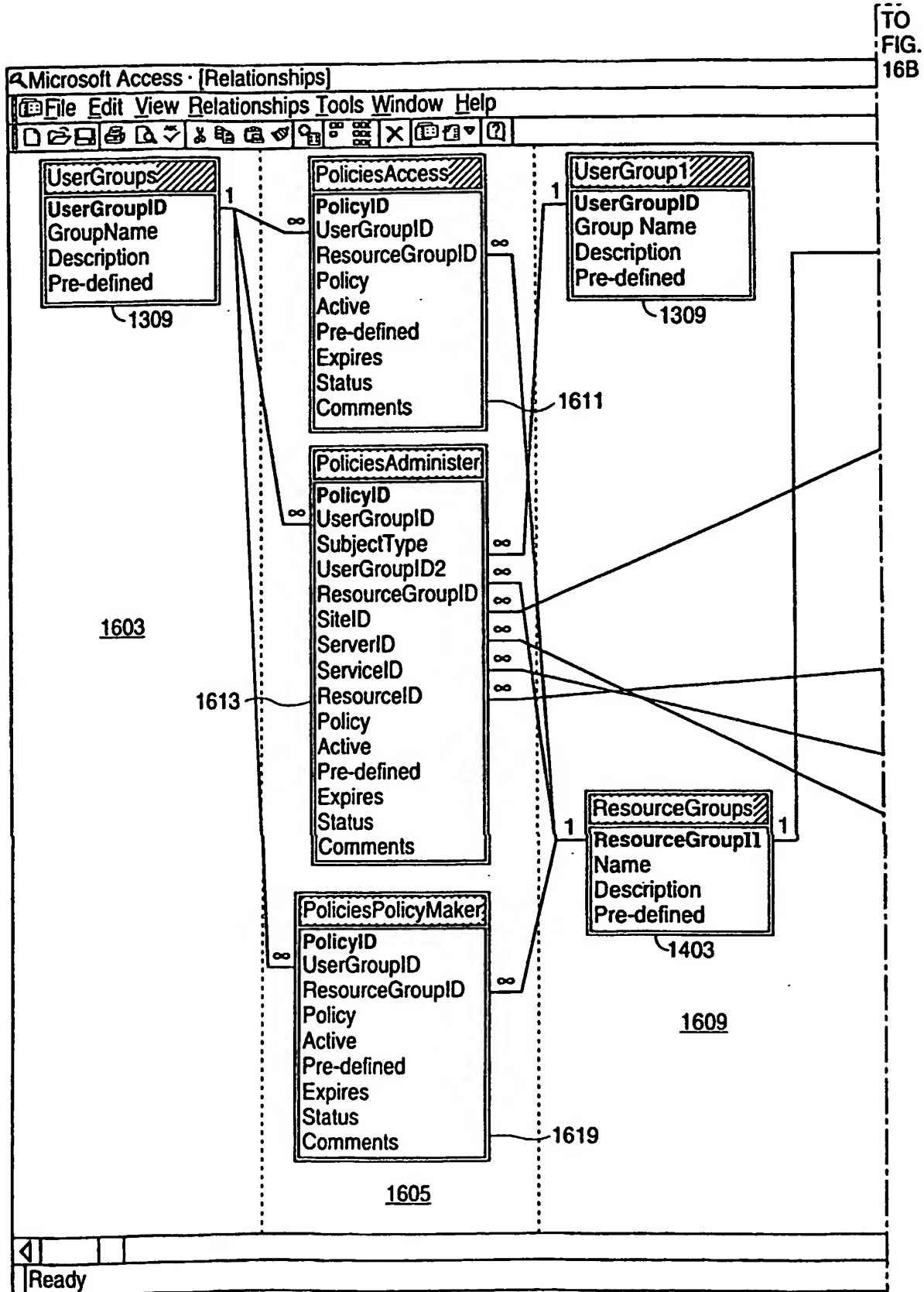


Fig. 15



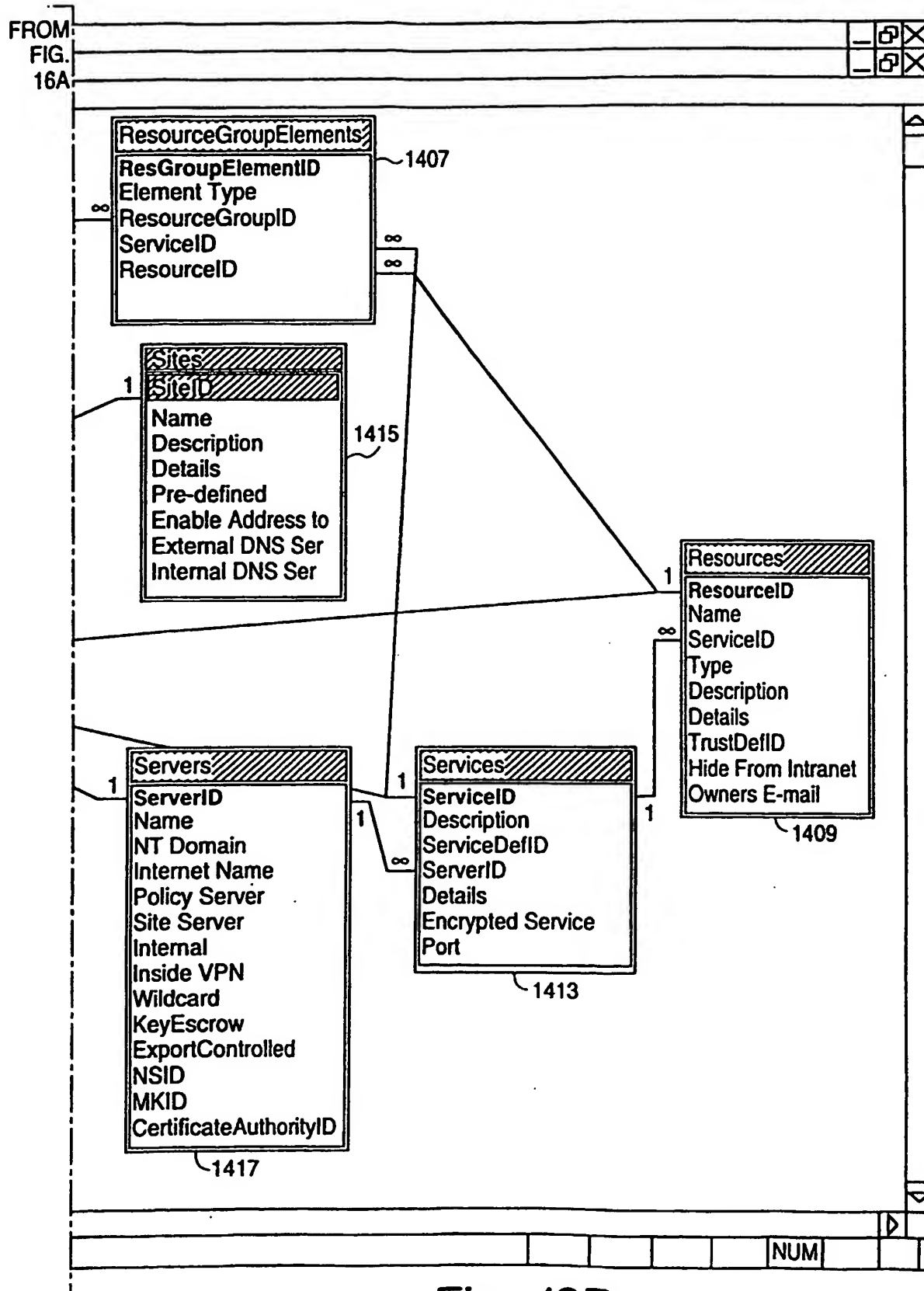
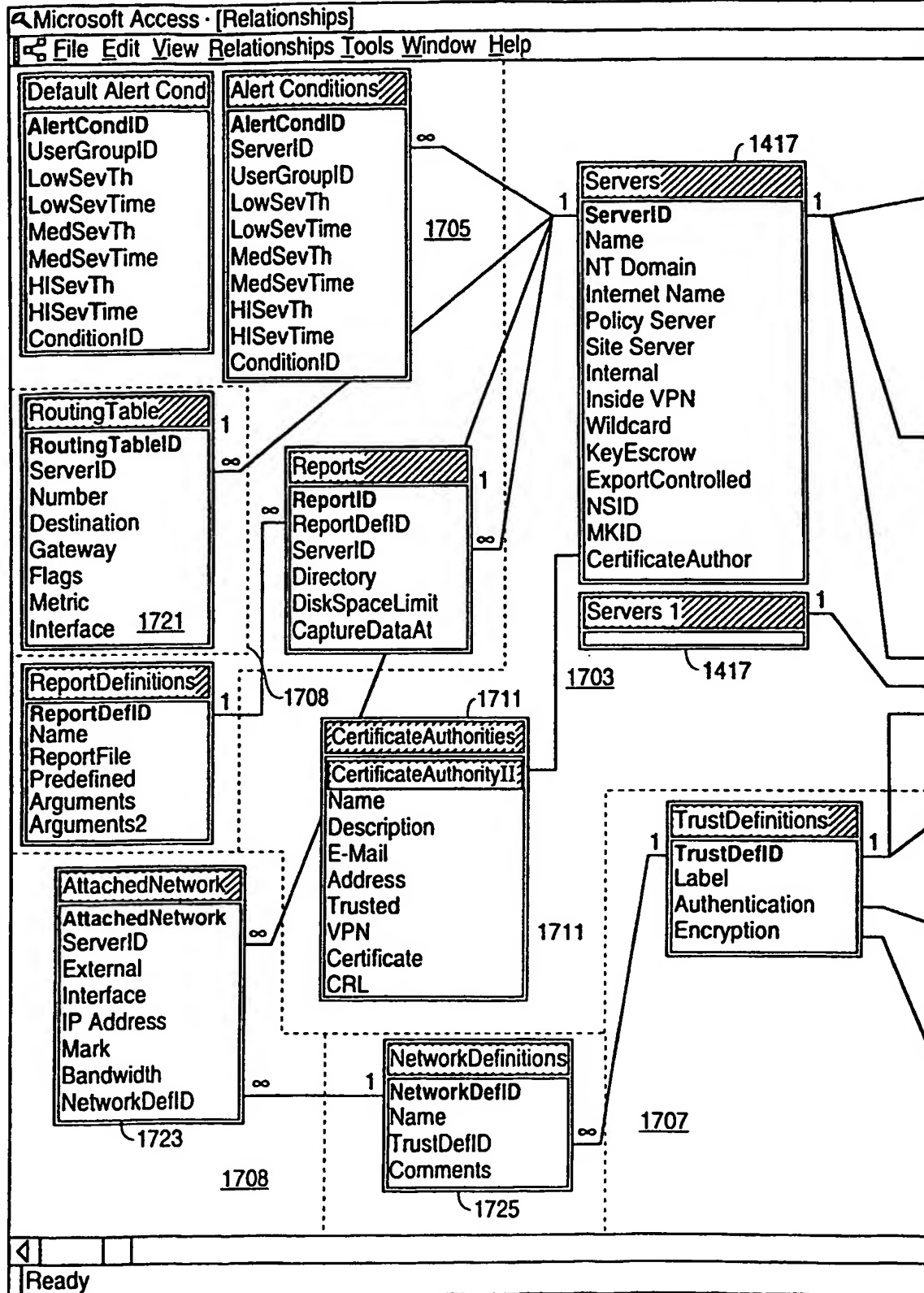


Fig. 16B

TO
FIG.
17B

10019101.122001

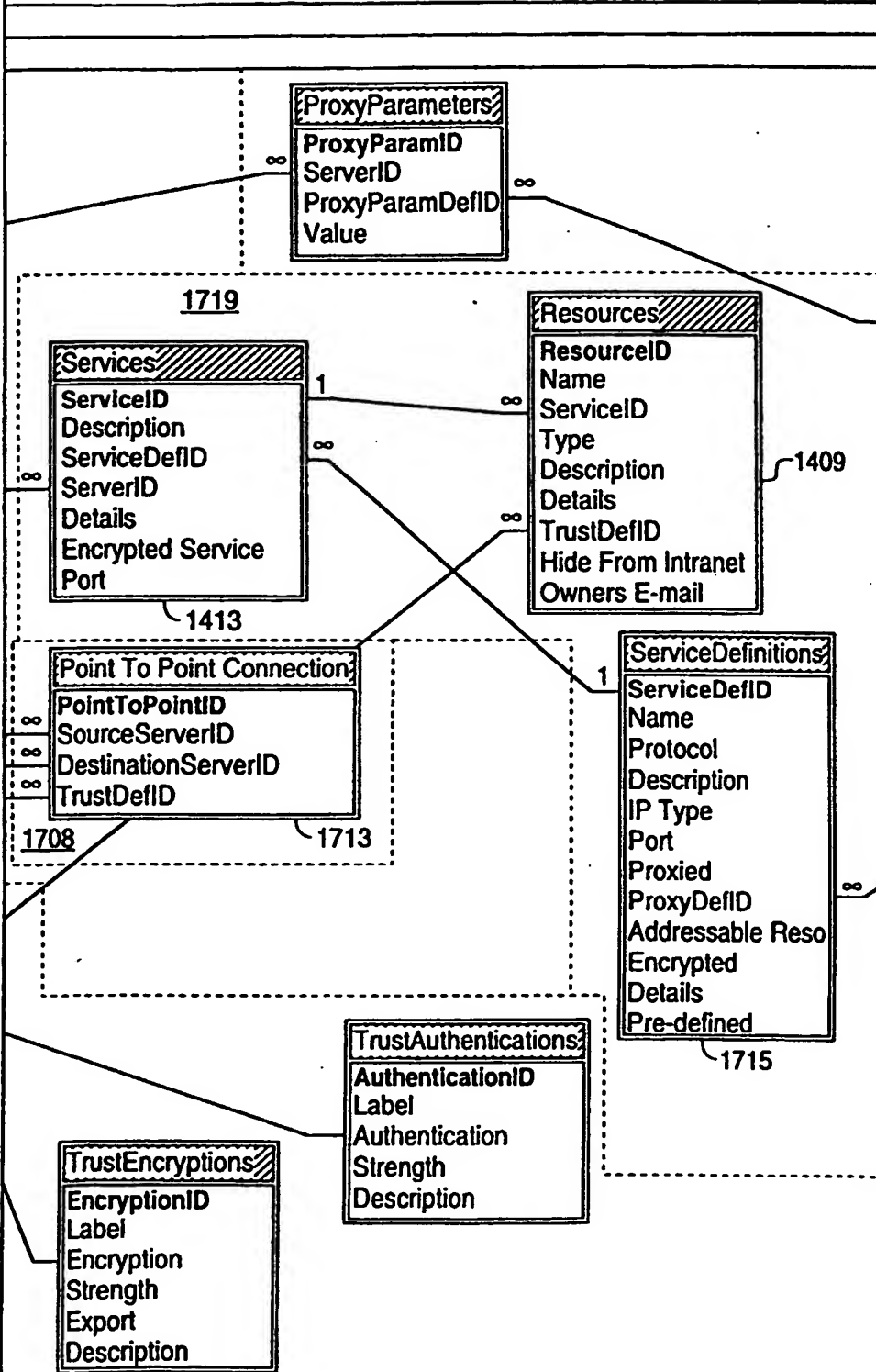
FROM
FIG. 17ATO
FIG. 17C

Fig. 17B

10049101.12004

FROM
FIG. 17B

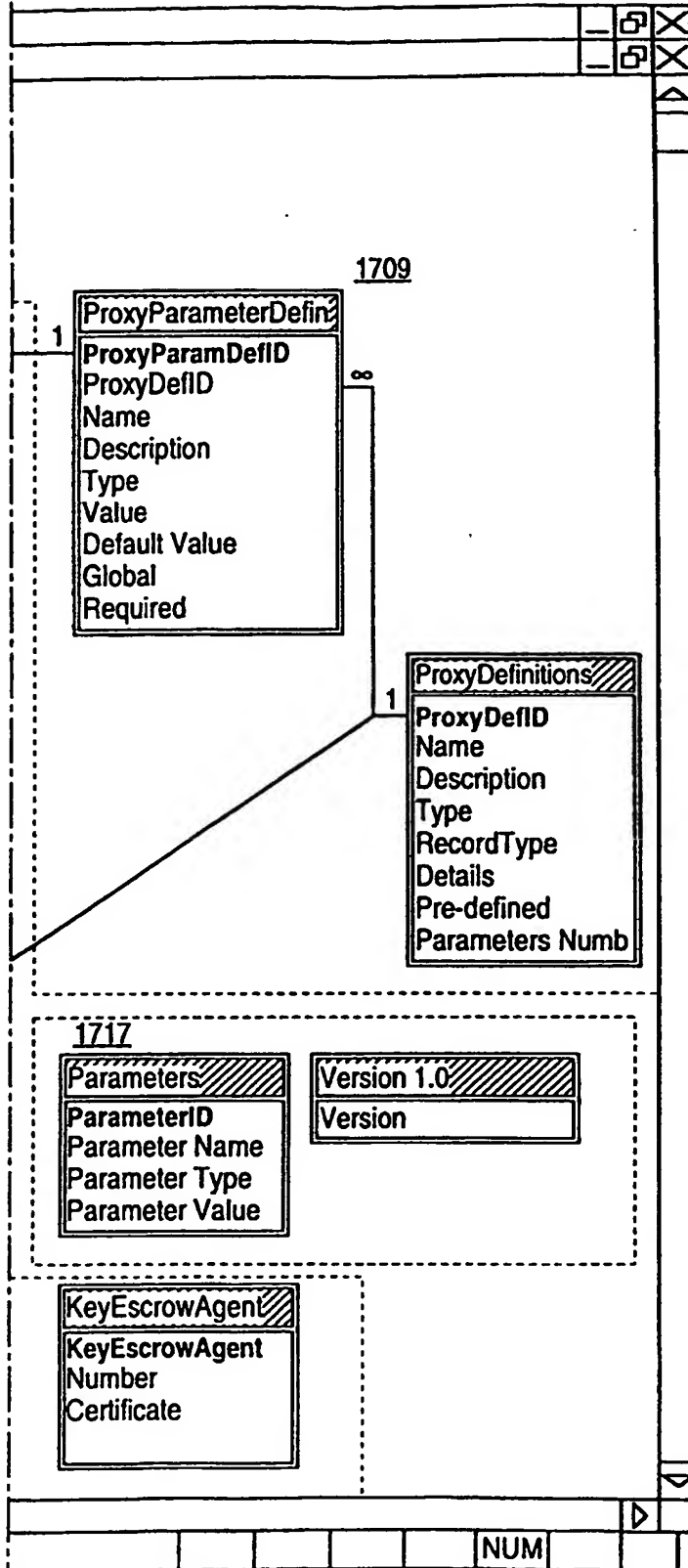


Fig. 17C

10019101-122004

▷ NARROWER ◁ WIDER ▽ SHORTER △ TALLER

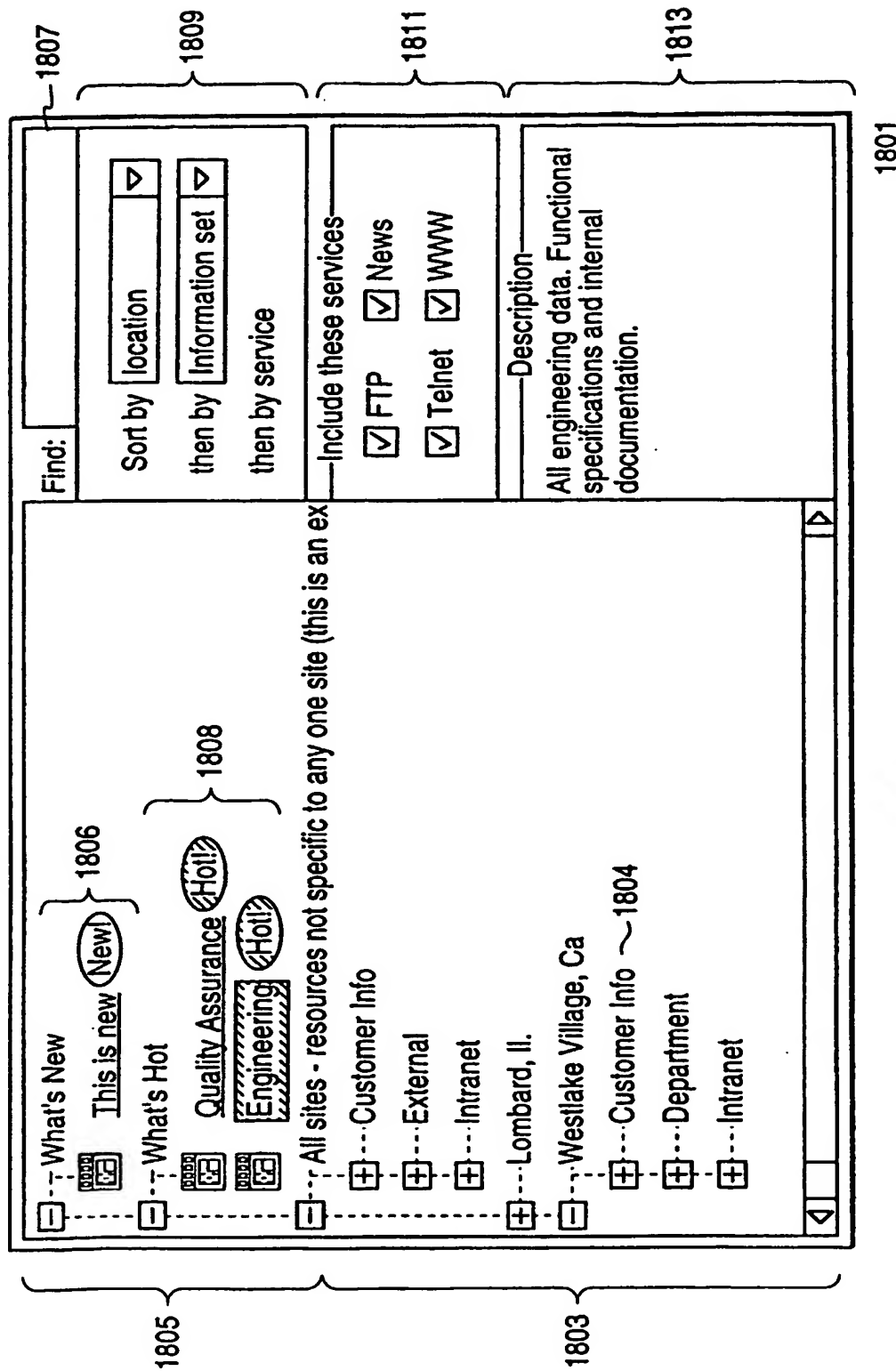


Fig. 18

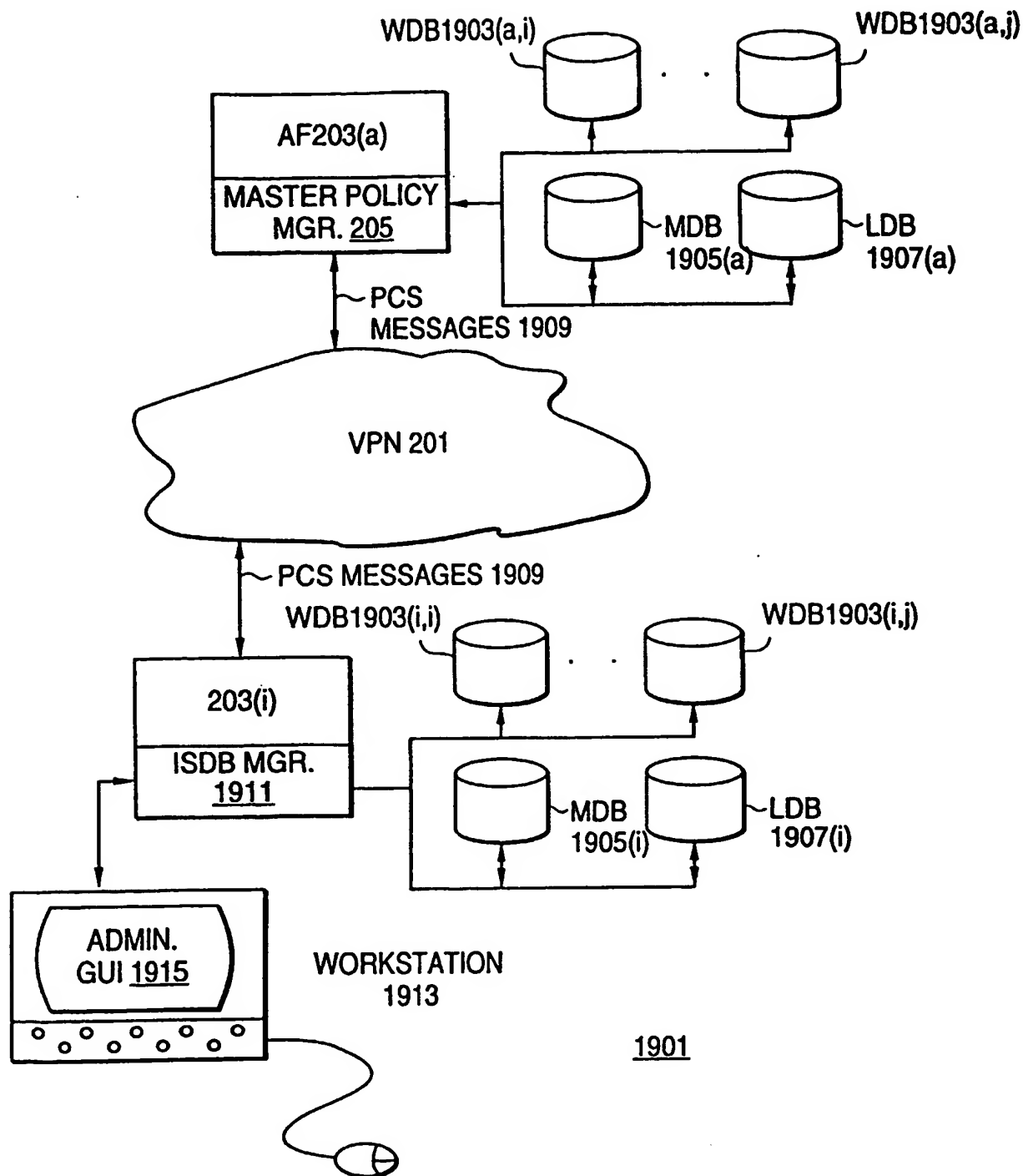
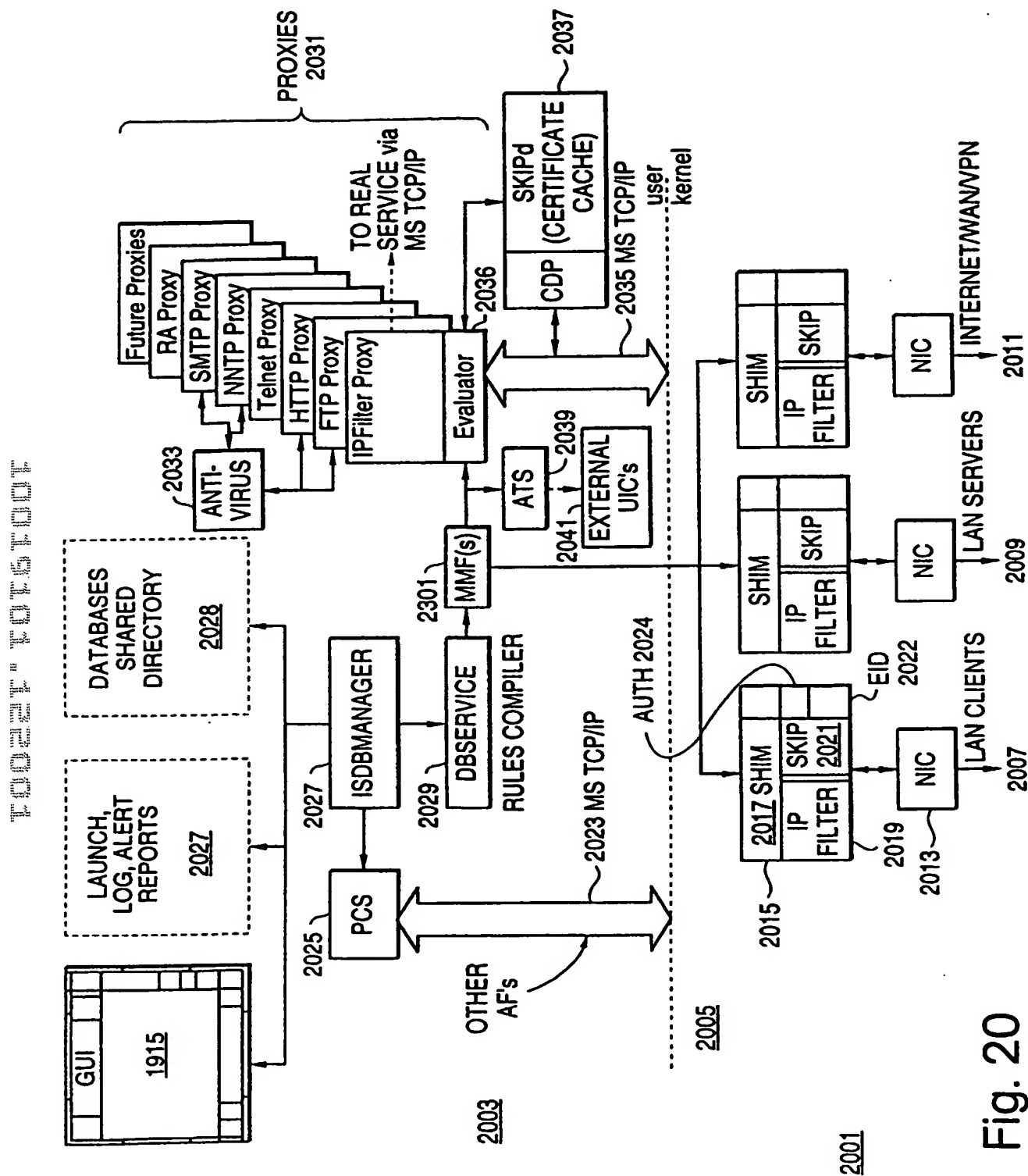
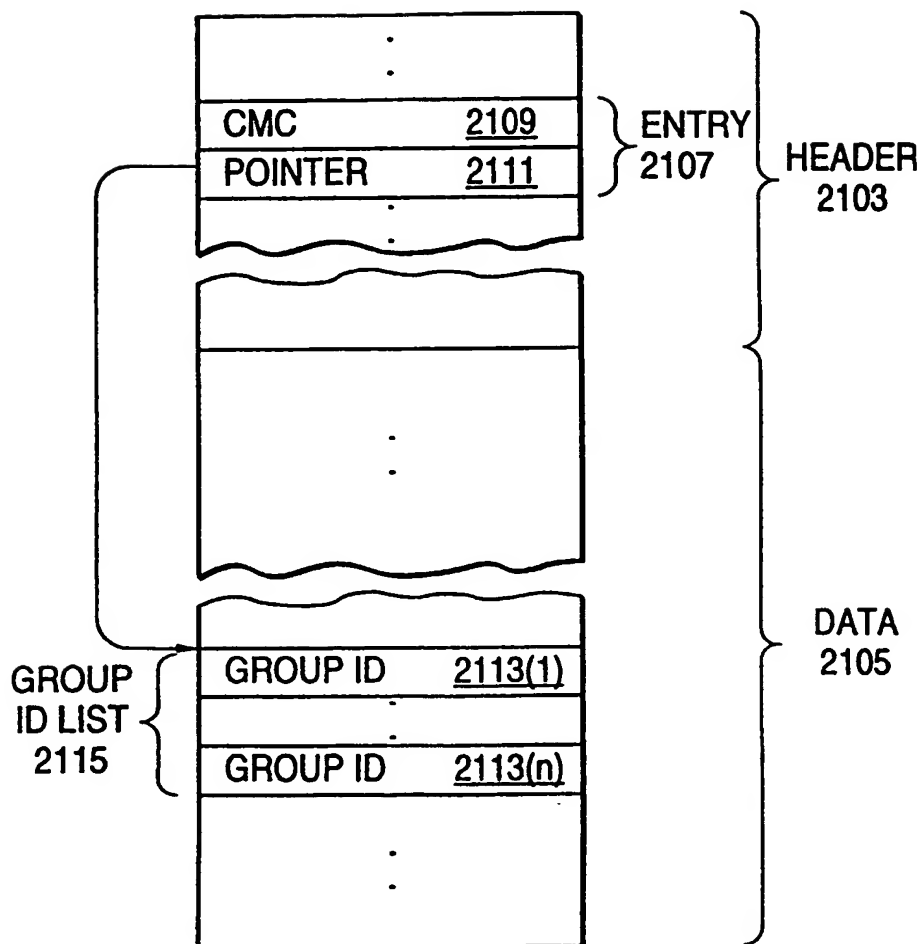


Fig. 19





DB CERTIFICATES BY
USER GROUP FILE 2101

2303

Fig. 21

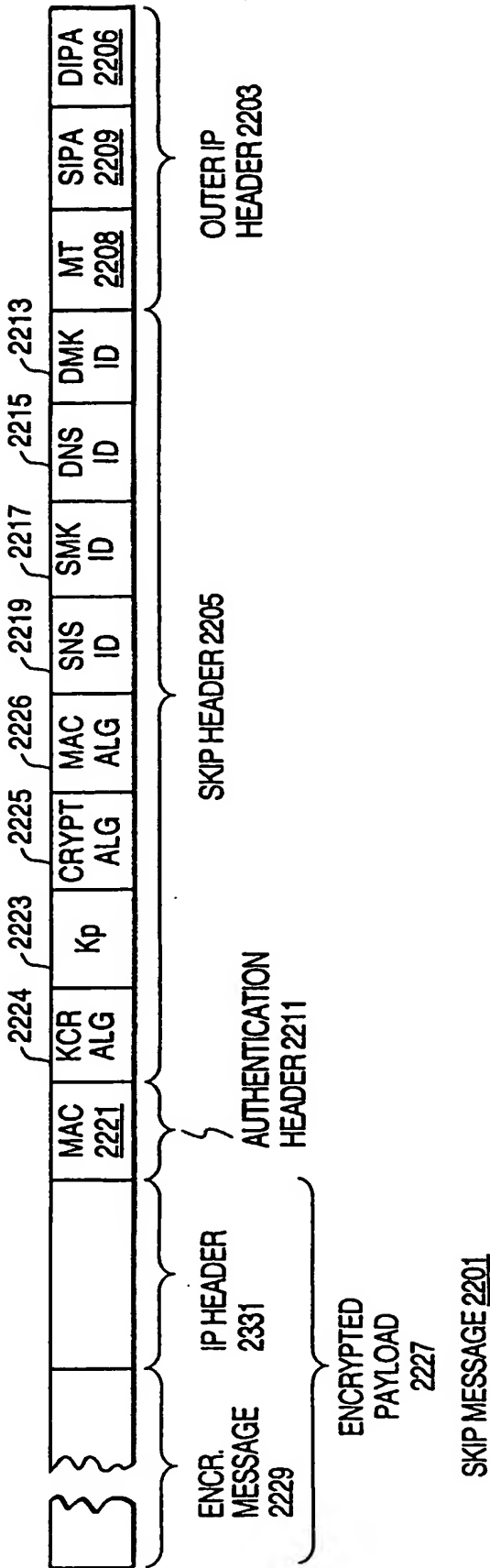


Fig. 22

File 2303 {

MMF File Name	Contents
	Policies, User Groups, and Information Sets 2305
DBUsersFile 2307	Describes policy application from the User Group viewpoint. Maps each DB UserGroupID to a list of ResourceGroupIDs with flags that indicate whether the policy that relates each pair is an allow or deny policy.
DBUsersTreeFile	Describes the user groups tree as a flattened array. Maps each DB UserGroup ID to a list of UserGroupIDs for parent user groups
DBResourcesFile 2309	Describes policy application from the Resource Group (information set) viewpoint. Maps each DB ResourceGroupID to a list of UserGroupIDs with flags that indicate whether the policy that relates each pair is an allow or deny policy.
DBResourcesTreeFile	Describes the resource groups tree as a flattened array. Maps each DB ResourceGroupID to a list of ResourceGroupIDs for parent information sets.
	User Identification Information 2311
DBIPRangesFile	IP Ranges data. Maps from IPRangeDefID to the IP range data.
DBDomainsFile	IP Domain data. Maps from DomainDefID to the IP domain data.
DBCertificatesFile	Certificate data. Maps from CertificateDefID to the certificate data.
DBWindowsIDFile	Windows ID data. Maps from WindowDefID to the windows ID data.
DBSmartCardIDFile	Smart card (authentication token) data. Maps from Smartcard-DefID to the authentication token data.
DBIPRangesByUserGroup File	Relates IP range matching criteria to user groups. Maps from IP Range data to UserGroupIDs.
DBDomainsByUserGroup File	Relates IP domain matching criteria to user groups. Maps from IP Domain data to UserGroupIDs.
DBCertificatesByUserGroup File	Relates certificates to user groups. Maps from certificate data to UserGroupIDs. 2101
DBWindowsIDByUserGroup File	Relates Windows IDs to user groups. Maps from Windows ID data to UserGroupIDs.
DBSmartCardIDByUser GroupFile	Relates Smart Card (authentication token) data to user groups. Maps from authentication token data to UserGroupIDs

2301

Fig. 23A

MMF File Name	Contents
	Servers, Services, and Information Resources 2313
DBResourcesByServerIDFile	Relates servers to resources. Maps from ServerIDs to ResourceIDs for resources held on the server identified by the ServerID.
DBResourcesByServiceIDFile	Relates services to resources. Maps from ServiceIDs to ResourceIDs for resources belonging to the service identified by the ServiceID.
DBResourceIDByServiceIDFile	Relates services to their information resources. Maps from ServiceID to ResourceID.
DBResourceIDByNameFile 2315	Relates the IP names (URLs) of resources to resource IDs. Maps from URL to resource ID.
DBResourcesByResourceIDFile 2317	Relates resources to information sets. Maps ResourceID to Resource GroupIDs.
	Servers, Services, IP Information, and Proxies 2319
DBServerIDByIPFile	Relates IP addresses to servers. Maps IP addresses to ServerIDs.
DBServerIDByNameFile	Relates IP names to servers. Maps the IP FQDN (fully qualified domain name) for each server to its ServerID.
DBIPAndTypeByServerIDFile	Relates servers to their locations inside or outside to the VPN. Maps ServerID to the server's IP address and a flag indicating whether the address is inside or outside the VPN.
DBServiceIDByPortFile	Relates services to their port numbers. Maps from ServiceID to port number.
DBServiceIDByServerIDFile	Relates servers to ports for services. Maps from ServerID to a list of port numbers.
DBServicePortToProxyPortFile	Relates service ports to the ports for their proxies. Maps from service port number to proxy port number.
DBProxyIDByServerIDFile	Relates servers to service proxies. Maps from ServerID to ProxyDefID.
DBProxyParametersFile	Relates proxies to configuration data for the proxies. Maps from ProxyDefID to options data

2301

Fig. 23B

MMF File Name	Contents
	Access Filter Information 2321
DBAttachedNetworksByIPFile	Relates network interfaces in the access filters to information for the interfaces. Maps from the interface's IP address to interface information.
DBAttachedNetworksByServerIDFile	Relates access filters to their network interfaces. Maps from ServerID for the access filter to interface information.
DBRoutingTableFile	Describes the IP routing information for all of the access filters. One block of information.
DBRoutingTableByServerIDFile	Relates access filters to their IP routing information. Maps from ServerID for the access filter to IP routing information.
DBPointToPointFile	Relates a point-to-point description of a network path to data for the path. Maps from PointToPointID for the path to the associated data.
	SEND Information 2323
DBTrustTableFile <u>2325</u>	Implements the SEND table. Maps from TrustDefID, indicating a trust level, to AuthenticationIDs for user identification techniques and EncryptionIDs for encryption techniques.
DBCertificateAuthoritiesFile	Relates identifiers for certificate authorities to their data. Maps from CertificateAuthorityID to associated data.
DBTrustAuthenticationsFile	Relates AuthenticationIDs to information about identification techniques. Maps from AuthenticationID to identification technique information.
DBTrustEncryptionsFile	Relates EncryptionIDs to information about encryption techniques. Maps from EncryptionID to encryption type and strength information.
	IntraMap Information 2422
DBJavaSiteTable	Maps from names of locations to LocationIDs.
DBJavaResourceTable	Maps from URLs of resources to their ResourceIDs, LocationIDs, and <i>hidden</i> flags.
DBJavaResourcesSetTable	Maps from names of information sets to ResourceGroupIDs, a list of ResourceIDs for all resources contained in the information set, and a list of ResourceGroupIDs for all of the information set's parents.

2301

Fig. 23C

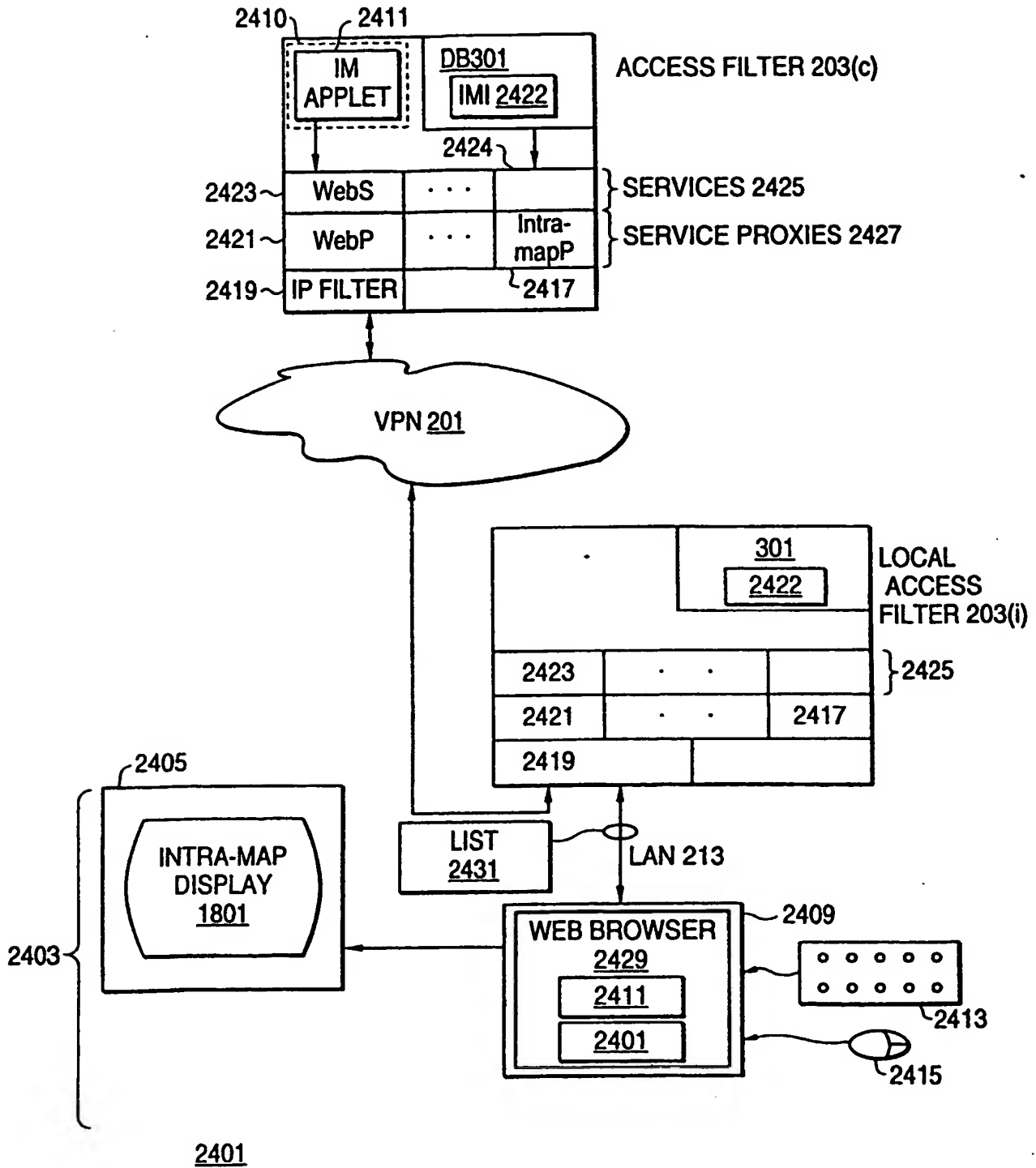


Fig. 24

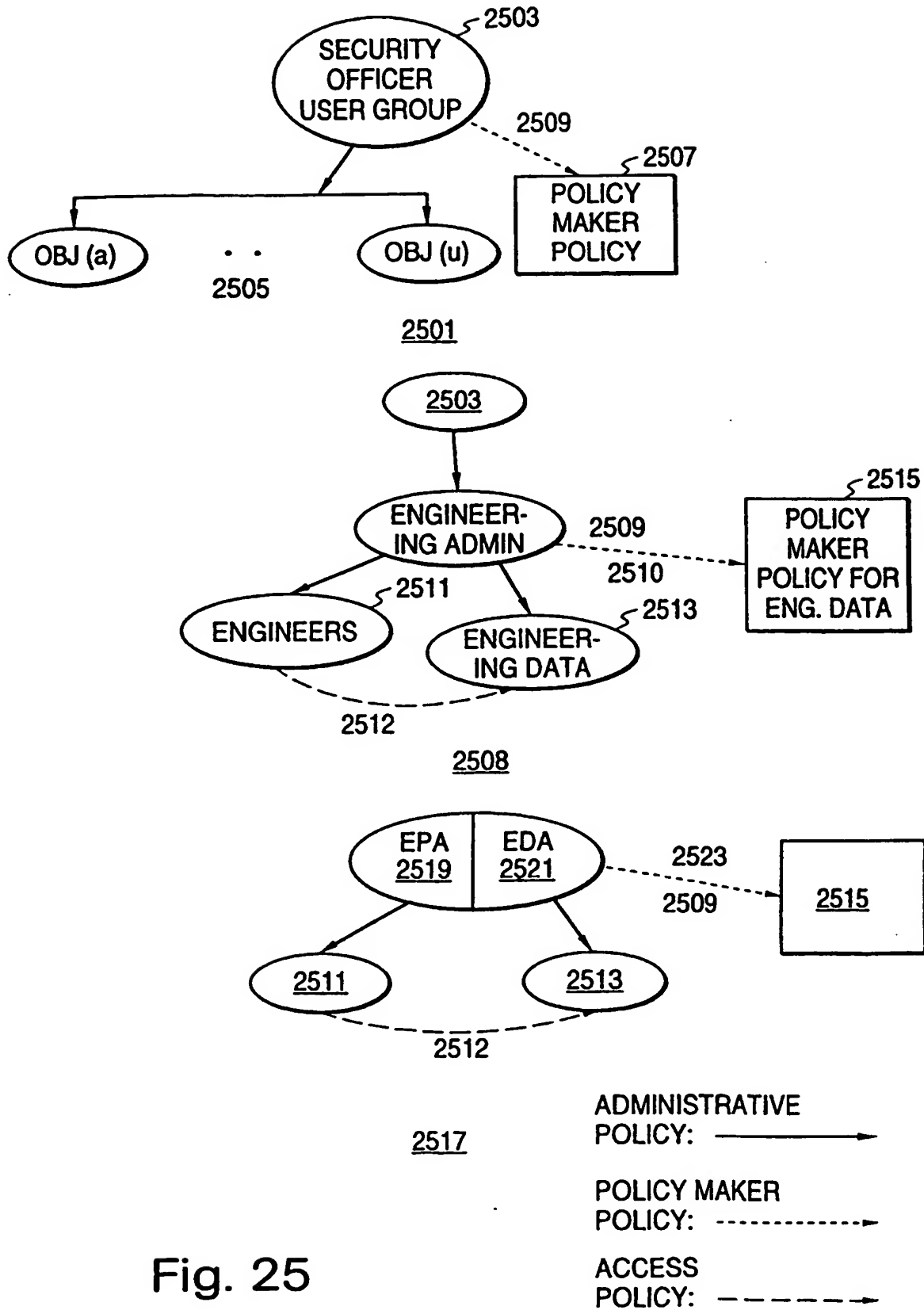


Fig. 25

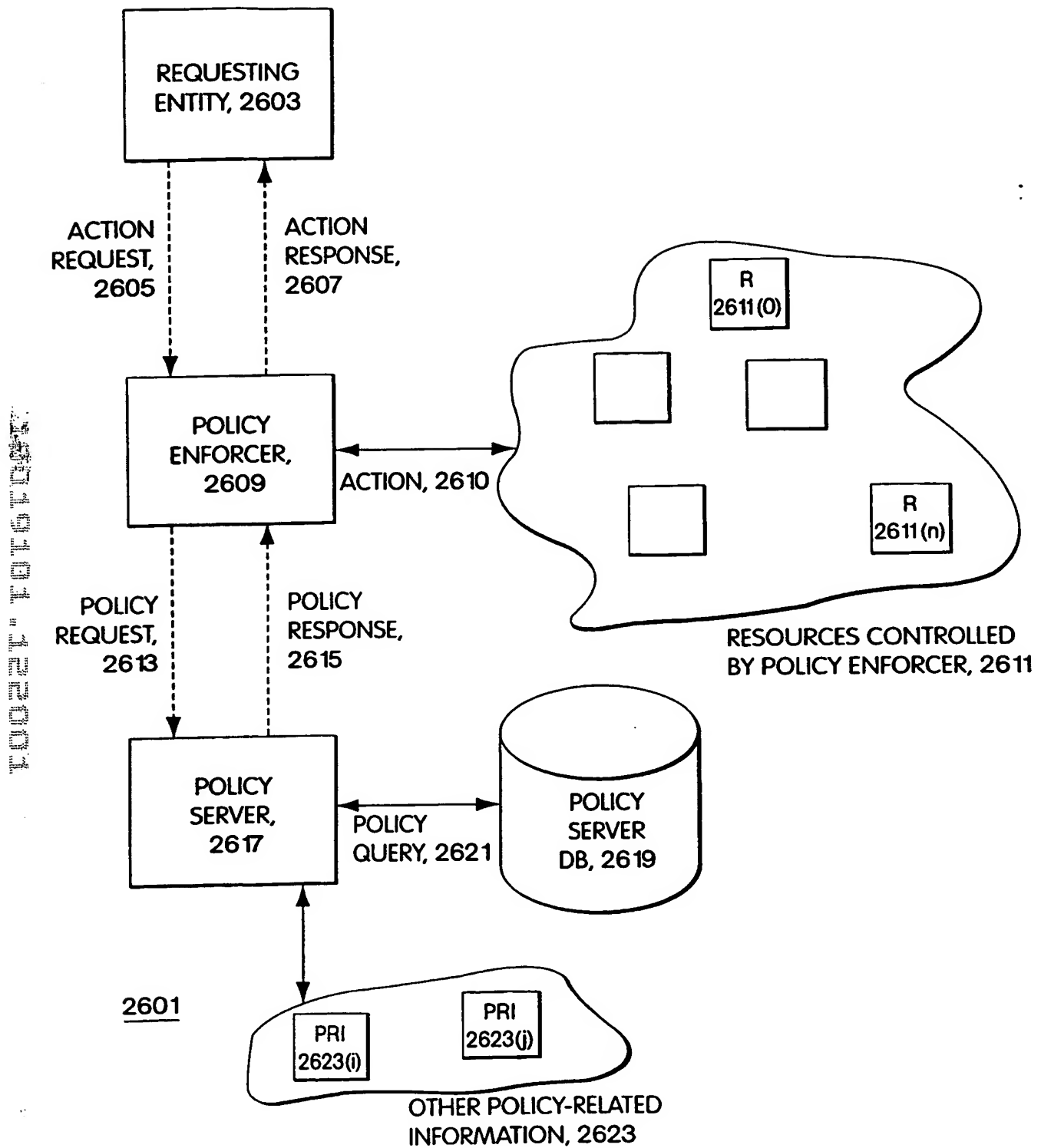
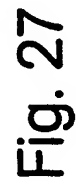


Fig. 26



2803
Entity [is | are] [allowed to | denied] *Action* [to | to the] *Resource*
[from | on | during] *TimeInterval(s)* [with | when] *ActionAttribute(s)*
2809 2811
2801

Fig. 28

10019101-122001

POLICY, 303

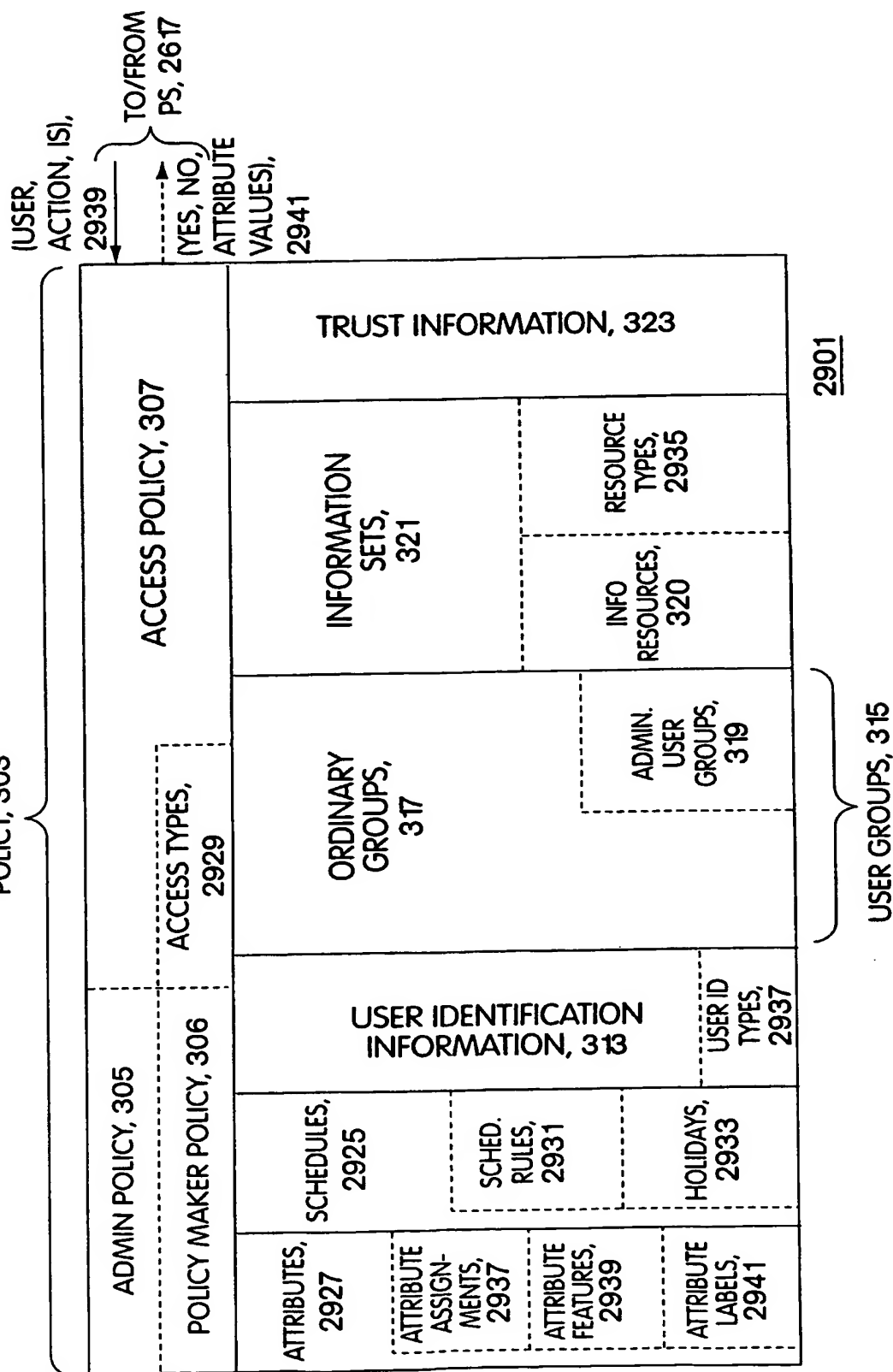


Fig. 29



Fig. 30

Conclave Administrator-ebola

Apply

Auth

Session

Copy

Paste

Find

Select

Sort

Sort

Expand

Collapse

Options

Exit

Help

+ New

X Delete

Properties

Main

User Groups

Information Sets

Policies

Schedule

QoS

Access Filters

Reports

AlertViewer

Schedules:

Business Hours

Non-working hours

5:00 PM-9:00AM Days:-MTWTF--

Days:-S---SH-

Weekends & Holidays

Workdays - Day Shift

Workdays - Graveyard Shift

Workdays - Swing Shift

3105

Rules:

Times Active

1:00 AM-9:00AM

5:00 PM-1:00AM

5:00 PM-9:00AM

9:00 AM-5:00PM

All day

Days Active

-MTWTF-X

-MTWTF-X

-MTWTF--

-MTWTF-X

S---SH-

Weeks Active

All

All

All

All

All

Months Active

All year

All year

All year

All year

All year

Description

Mon-Fri 1am - 9am

Mon-Fri 5pm - 1am

Mon-Fri 9am - 5pm

Weekends & Holidays

3107

3109

3111

3103

3106

3102

Fig. 31

10/019101

Schedule Rule [X]

Schedule Valid: _____

☐ All Day 3203

☒ Starts: 5:00 PM Ends: 9:00 PM

On selected days of week:

☒ Mo ☒ Tu ☒ We ☒ Th ☒ Fr ☐ Sa ☐ Su

☒ Weekdays 3205 ☐ Weekends

☐ Exclude Holidays ☐ Holidays

☒ Every week 3207

☐ Every 2 Weeks starting on 6/23/99

☐ On selected week of month:

☐ 1st ☐ 2nd ☐ 3rd ☐ 4th ☐ Last

☒ All year 3209

☐ On selected months

☐ Jan ☐ Feb ☐ Mar ☐ Apr ☐ May ☐ Jun

☐ Jul ☐ Aug ☐ Sep ☐ Oct ☐ Nov ☐ Dec

Description

3211

OK
Cancel
Holidays
Help
Advanced <<

3201

Fig. 32

Policy Properties [X]

User Group: Corporate [OK]

Information Set: Corporate [Cancel]

Policy: ☒ Allow ☐ Deny

State: ☒ Active ☐ Inactive

Apply All

Help

Comment: ! Corporate access to corporate information [Advanced <<]

Valid Between:

☐ Start Date []

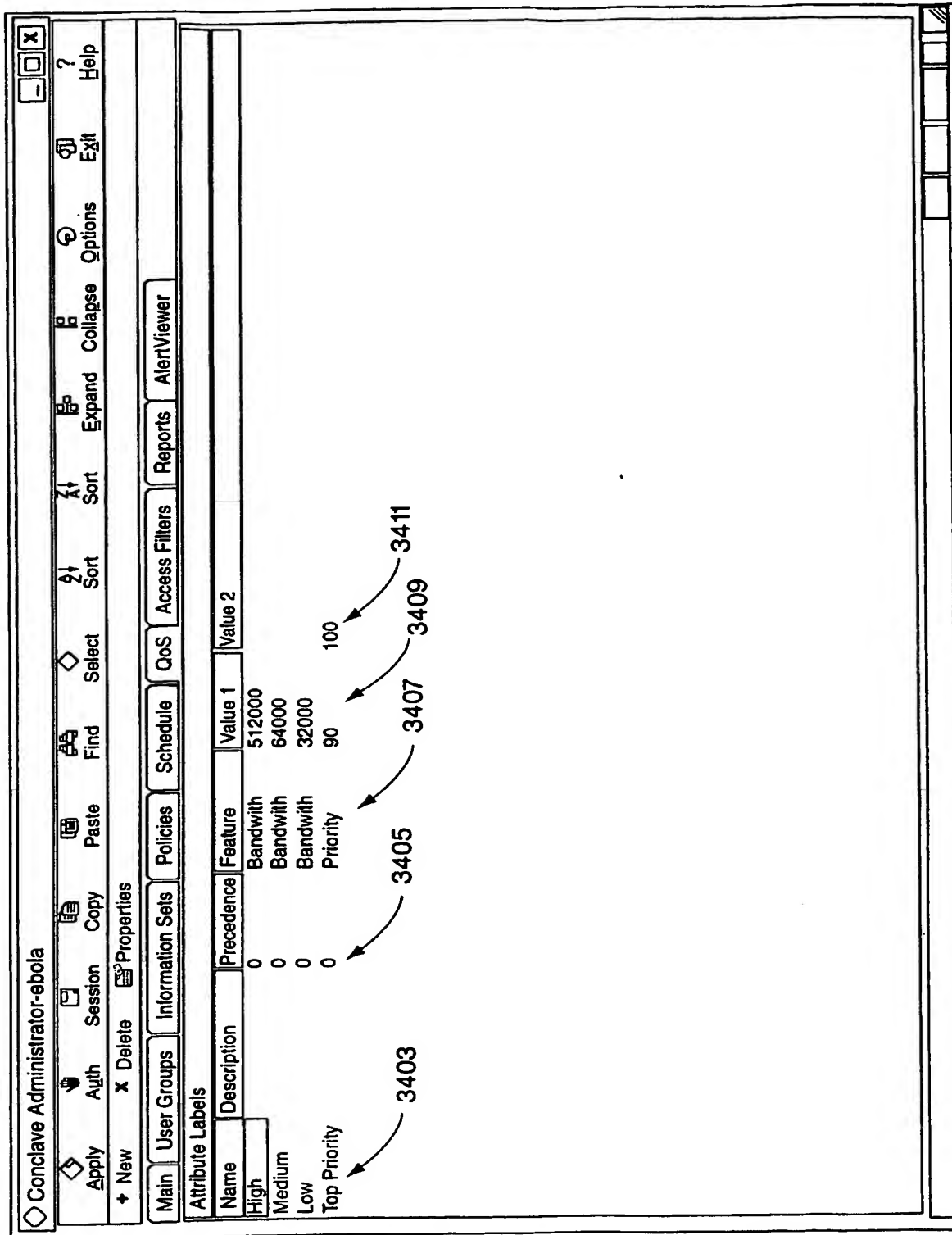
☐ End Date []

Schedule Name: Business Hours [] [Definition]

3303 3305

3301

Fig. 33



3401

Fig. 34

Conclave Administrator-ebola

Apply Auth X Delete Properties Evaluation Clear 16/23/89 11:04 AM

Find Select Sort Expand Collapse Options Exit Help

User Groups Information Sets Policies Schedule QoS Access Filters Reports AlertViewer

Access Policies Administrative Policy Maker QoS Assignments

Active User Groups QoS Definition Subject

Medium

High

Low

High

3507

Finance

Service Type: Web

Service Type: File Trar

Service Type: Remote

Finance

3505

3509

3511

3503

User Groups

Administrative

Internet

Intranet

Intranet IP Users

VPN Users

Conclave Services Users

Departments

Locations

System Services Users

3513

Subject

Information Sets Available Information Services

Customer Information

Internet

Allowed

Internet Mail Service

Internet Sites

Intranet

Conclave Services

Departments

Employees

Public

System Services

3515

3501

Fig. 35

Attribute Label [X]

Attribute Label

Attribute Label:

Description:

Label Precedence:

Associated Feature

Feature: ▾

Value 1:

Value 2:

3607

3605

3601

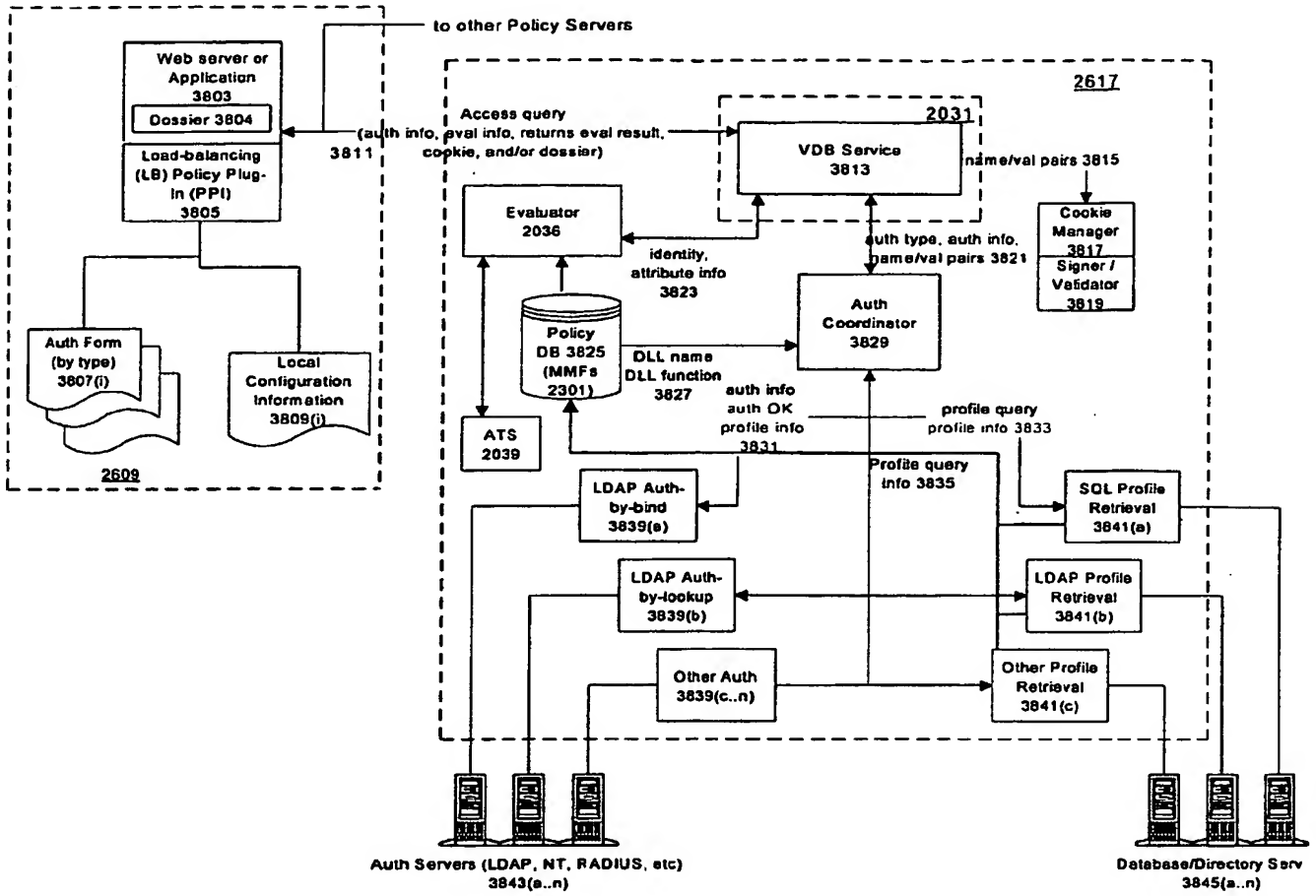
Fig. 36

Attribute Feature [X]

Class:	3703	Quality of Service	▼	OK
Name:	3705	Priority		Control
Description:	3707	Bandwidth Priority		Help
Value Type:		Pair	▼	3709
Feature Precedence:		0		3711
Value Precedence:		0		
Restrictions:		None	▼	3713

3701

Fig. 37



3801

FIG. 38

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD W3 HTML//EN">
<html>

<head>
<meta content="text/html; charset=unicode" http-
equiv="Content-Type">
<!-- #include file="psquery.inc" -->
<title>Policy Query Example</title>
</head>

<body>

<h1>Conclave Policy Enabled Page</h1>
<%
  if ConclavePolicyAllowed() = "Yes" then
    'Put the allowed action here
    Response.Write "<p>You've been allowed to this
page.</p>"
  else
    'Put denied action here
    Response.Write "<p>You've been <b>denied</b> to this
page.</p>"
  end if
%>

<p>&nbsp;</p>
</body>
</html>

```

3903

3905

3907

3901

FIG. 39

```

<#
'#####
'% File:      psquery.inc
'%           Perform Policy Server
'%           Query against the current page
'#####
Function ConclavePolicyAllowed()
    dsn = "ConclavePolicyServer"
    dbuser = "anyone"
    dbpass = "anything"
} 4003

'default to not allowed
ConclavePolicyAllowed = "No" } 4005

'Get the session variables for the query
sourceIP = Request.ServerVariables("REMOTE_ADDR")
destIP = Request.ServerVariables("LOCAL_ADDR")
destPort = Request.ServerVariables("SERVER_PORT")
resource = Request.ServerVariables("URL")
} 4007

'remove any prepended slash on the URL
if left(resource,1) = "/" then
    if resource <> "/" then
        resource = mid(resource, 2)
    end if
end if

'Construct the SQL query
dbsql = "SELECT IsAllowed FROM PolicyEval WHERE"
        & " SourceIP = '" & sourceIP & "'"
        & " AND DestinationIP = '" & destIP & "'"
        & " AND SourcePort = 0"
        & " AND DestinationPort = '" & destPort
        & " AND Resource = '" & resource & "'"
        & " AND IncludeIdentityStore='Y'"
        & " AND AskClientForIdentities='Y'"
} 4009

Set Conn = Server.CreateObject("ADODB.Connection")
Set rs = Server.CreateObject("ADODB.RecordSet")
Conn.Open dsn, dbuser, dbpass
} 4011

RS.Open dbsql, Conn 4013

if Conn.Errors.Count = 0 then
    if Not RS.EOF then
        ConclavePolicyAllowed = RS(0)
    end if
end if 4015

RS.Close
Set RS = Nothing
Conn.Close
Set Conn = Nothing
} 4017

End Function
#>

```

3903

FIG. 40

POLICYEVAL : Table		
	FieldName	Data type
410	IsAllowed	Text
410	PolicySet	Number
410	HasExpireTime	Text
410	ExpireTime	Binary
411	ExpireSeconds	Number
411	ReasonCode	Number
411	Reason	Text
411	Identity	Text
412	SourceIP	Text
412	DestinationIP	Text
412	SourcePort	Number
412	DestinationPort	Number
412	EncryptionAlg	Number
412	AuthenticationAlg	Number
413	IPProtocol	Number
413	EvalTimeStamp	Binary
413	Resource	Text
413	Application	Text
414	IncludeQoS	Text
414	IncludeSchedules	Text
414	IncludeIdentityStore	Text
414	IncludeVPNManager	Text
414	AskClientForIdentities	Text
415	AuthCode	Text
415	MaybeList	Text
415	AttributeName	Text
415	AttributeValue	Text
416	Cookie	Text
416	IdentityNumber	Number
416	IdentityType	Text
416	IdentityIsValid	Text
416	IdentityAuthStatus	Number
416	IdentityAuthStatusDesc	Text

4101

FIG. 41

```

SELECT IsAllowed, PolicySet, HasExpireTime, ExpireTime, Reason from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND SourcePort = 0
AND DestinationIP = '172.31.1.32'
AND DestinationPort = 80
AND EncryptionAlg = 64
AND AuthenticationAlg = 2
AND IPProtocol = 6
AND EvalTimeStamp = '07-JUL-1999 13:39:34'
AND Resource = 'Conclave/ConclaveEval.html'

```

4203

IsAllowed	PolicySet	HasExpireTime	ExpireTime	Reason
Y	56	N	1969-12-31 16:00:00	None

4205

4201

```

SELECT IsAllowed, Reason from PolicyEval
WHERE SourceIP = '172.31.1.31'
AND SourcePort = 0
AND DestinationIP = '172.31.1.32'
AND DestinationPort = 80
AND EncryptionAlg = 64
AND AuthenticationAlg = 2
AND IPProtocol = 6
AND EvalTimeStamp = '07-JUL-1999 13:39:34'
AND Resource = 'Conclave/ConclaveEval.html'

```

4209

IsAllowed	Reason
Y	None

4211

4207

```

SELECT * from PolicyEval
WHERE SourceIP = '172.31.1.31'
AND SourcePort = 0
AND DestinationIP = '172.31.1.32'
AND DestinationPort = 80
AND EncryptionAlg = 64
AND AuthenticationAlg = 2
AND IPProtocol = 6
AND EvalTimeStamp = '07-JUL-1999 13:39:34'
AND Resource = 'Conclave/ConclaveEval.html'

```

4213

```

SELECT IsAllowed, PolicySet, HasExpireTime, ExpireTime, Reason from PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'
AND Resource = 'Conclave/ConclaveEval.html'

```

4217

IsAllow ed	PolicySet	HasExpireTi me	ExpireTime	Reason
Y	56	N	1969-12-31 16:00:00	None

4219

4215

FIG. 42


```

SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'
AND Resource = 'Conclave/ConclaveEval.html'

```

4303

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4305

4301

```

SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'
AND Resource = 'Conclave/ConclaveEval.html'
AND IdentType = 'CertificateDN'
AND IdentValue = '/O=XYZ/OU=Engineering/CN=JoeUser'

```

4309

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4311

4307

```

SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'
AND Resource = 'Conclave/ConclaveEval.html'
AND IncludeIdentityStore = 'Y'

```

4315

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4317

4313

```

SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'
AND Resource = 'Conclave/ConclaveEval.html'
AND IncludeIdentityStore = 'Y'
AND IdentType NOT IN ( 'WindowsID', 'Radius', 'IP' )

```

4321

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4322

4319

FIG. 43

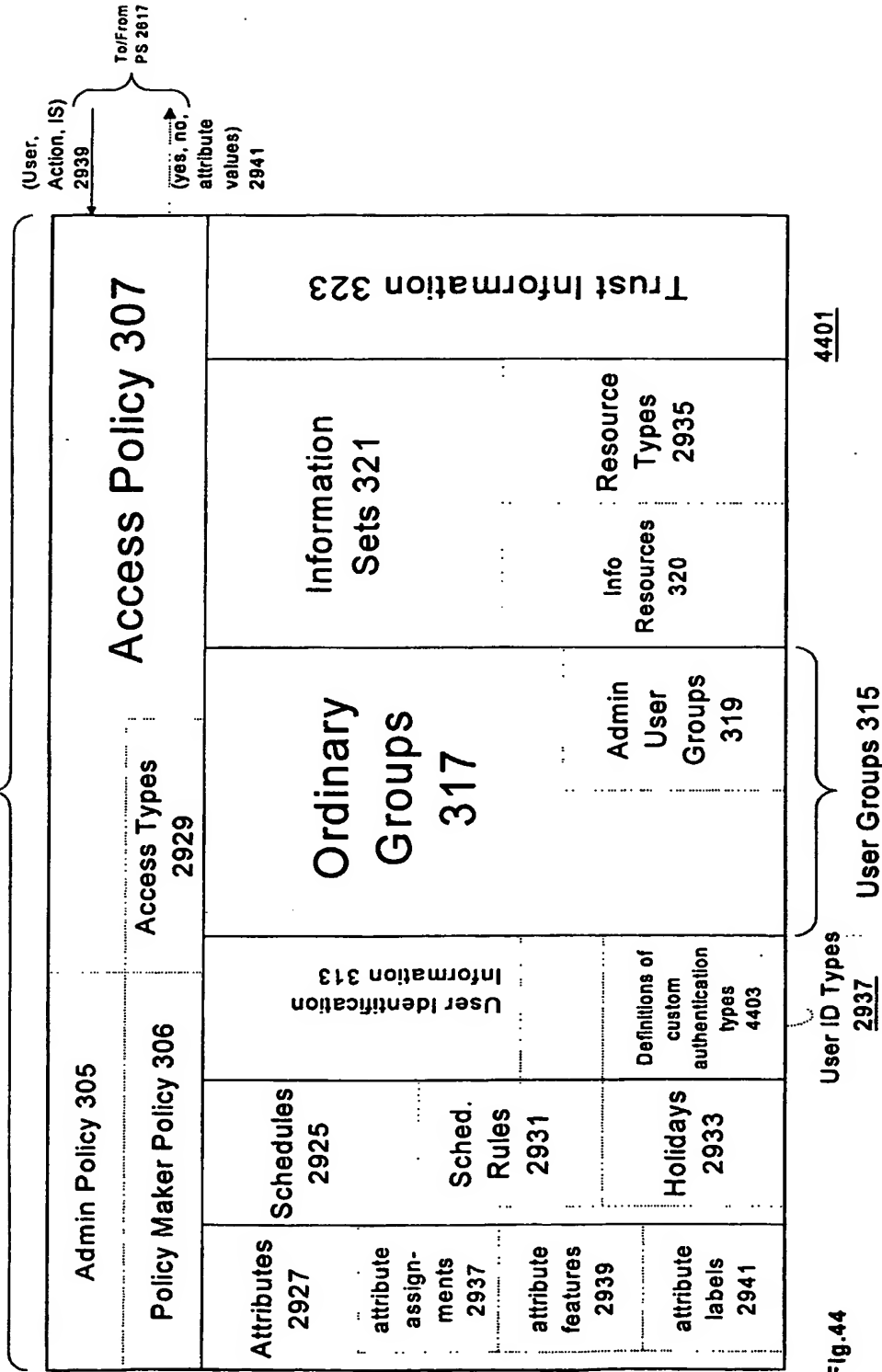
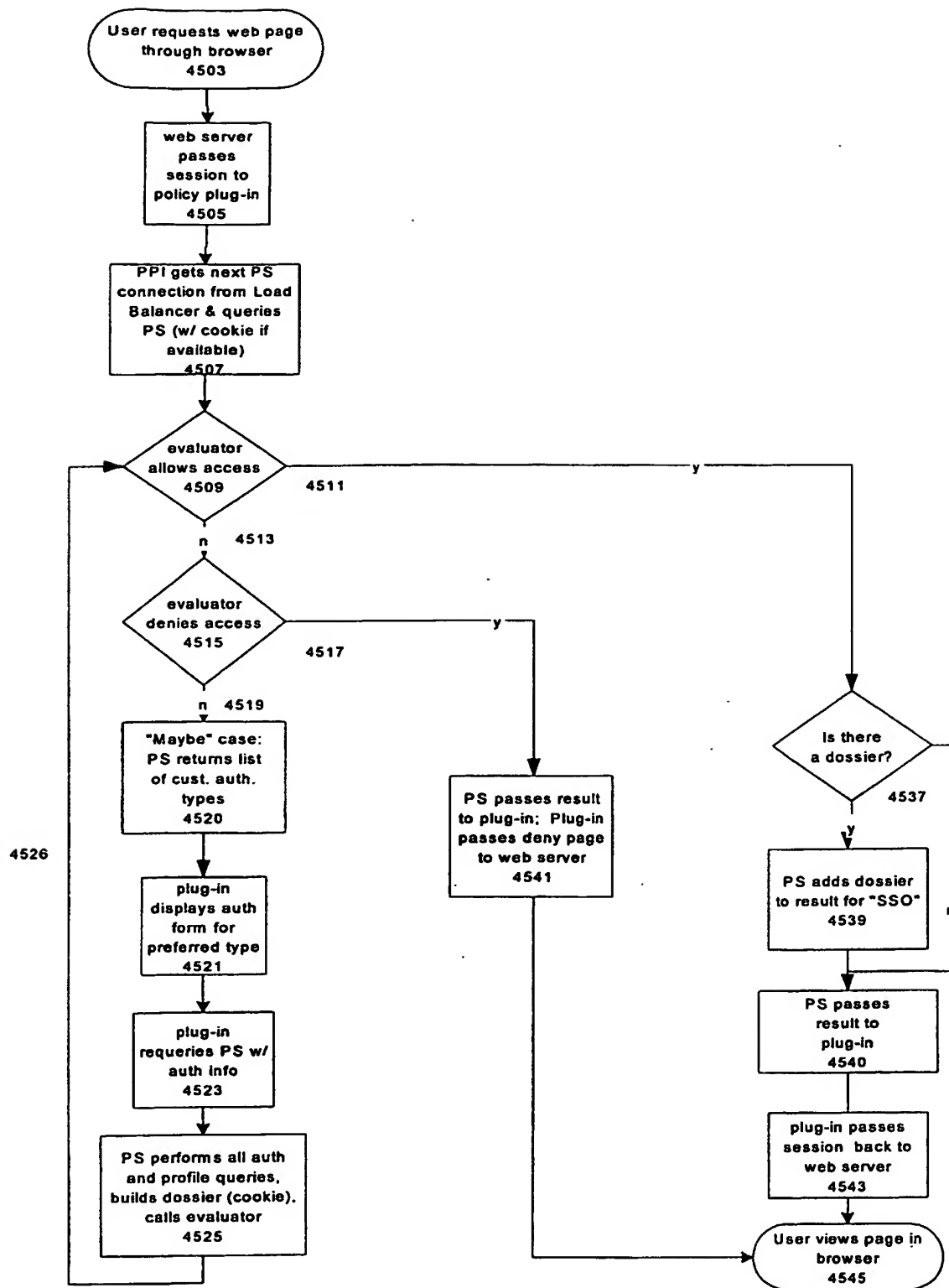


Fig.44



4501

FIG. 45

10049404.122004

4609

4611

Authentication Type Properties

LDAP Bind

Bind to directory as user logging in

2 hours

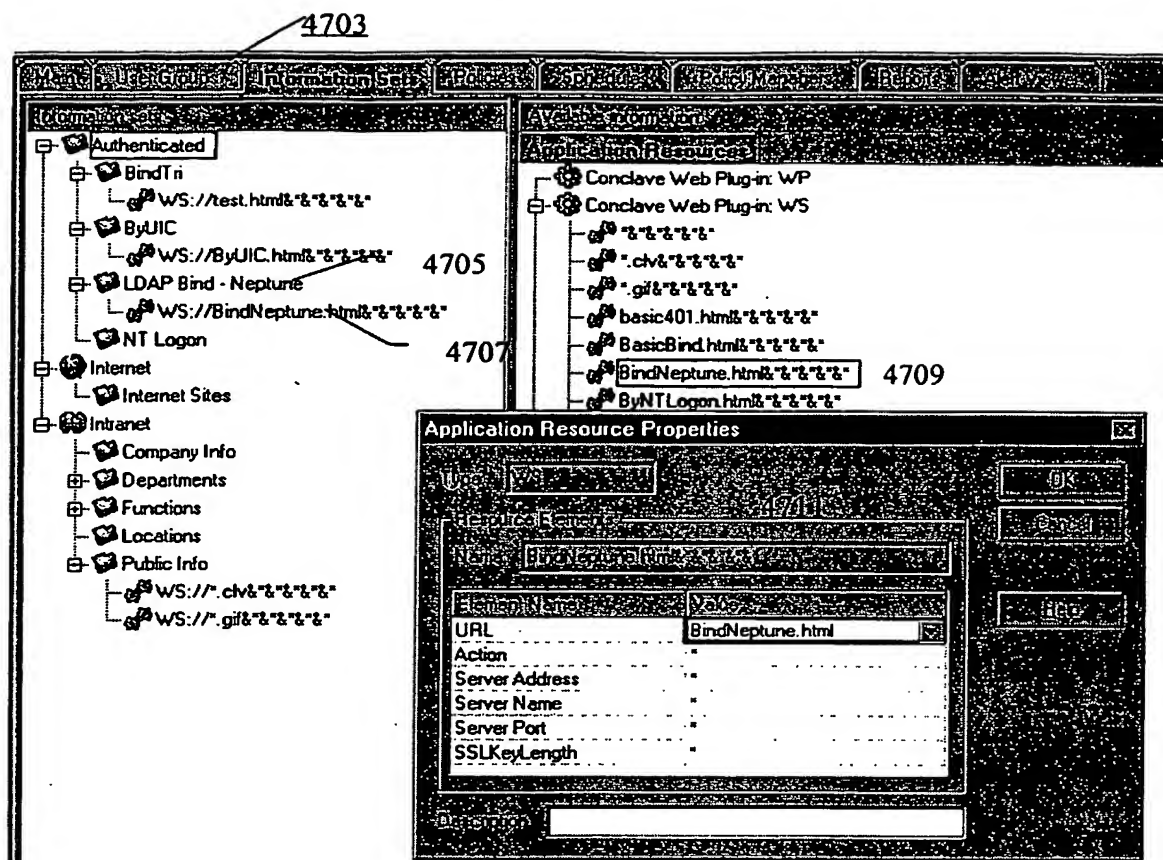
AuthByLDAPBind

ClientAuth.dll

Name	Value	Type	Description
AnonymousBindAllowed	N	string	
AnonymousSearch	N	string	
AttributeSearch		string	
DefaultSearchPrefix	cn		
Password	\$(PWD)	string	Form variable to use as password when binding to directory
Port	389	long	Port on which the directory is listening
SearchScope	subtree	string	Search type - one of: base, onelvel, subtree (base = exact)
Server	192.168.36.218	string	Name (FQDN) or IP Address of LDAP directory server
StartSearchFrom	cn=\$(USER),ou=QA,ou=Engineering,o=DI	string	Full DN to the node to start searching at
UserName	cn=\$(USER),ou=QA,ou=Engineering,o=DI	string	Form variable to use as user name when binding to directory

4601

FIG. 46



4701

FIG. 47

10/019101

10019101 "T06T00T"

The screenshot displays a software interface with a table and two tree views.

Table:

User Group	Access	Information Set	Emp	Schedule	StandData	EndData	Log
<input checked="" type="checkbox"/> Bind Triceratops	Allow	BindTri					
<input checked="" type="checkbox"/> Admin	Allow	Sales					
<input checked="" type="checkbox"/> ByUIC	Allow	ByUIC					
<input checked="" type="checkbox"/> Engineers	Allow	Admin	✓		4801		
<input checked="" type="checkbox"/> Internet	Allow	Public Info					DP02
<input checked="" type="checkbox"/> NT Logon	Allow	NT Logon	✓		4803		
<input checked="" type="checkbox"/> SalesPeople	Allow	Upload					
<input checked="" type="checkbox"/> Account Members	Allow	Basic401 Resources	✓				

Left Tree View (User Groups):

- Administrators
- Authenticated
 - LDAP Bind: Name="*, Attributes=telephoneNumber="
- Bind Neptune
- Bind Triceratops
- ByUIC
- NT Logon
- Internet
- Intranet
 - Departments
 - Functions
 - Intranet IP Users
 - Locations

Right Tree View (Information Set):

- Authenticated
 - BindTri
 - ByUIC
 - LDAP Bind - Neptune
 - WS://BindNeptune.html?*&*&*
 - NT Logon
- Internet
 - Internet Sites
- Intranet
 - Company Info
 - Departments
 - Functions
 - Locations
 - Public Info

Annotations:

- 4807 points to the "LDAP Bind: Name="*, Attributes=telephoneNumber=" entry in the left tree.
- 4805 points to the "Departments" entry under the "Intranet" node in the left tree.
- 4709 points to the "WS://BindNeptune.html?*&*&*" entry in the right tree.
- 4809 points to the "Company Info" entry under the "Intranet" node in the right tree.

FIG. 48

TABLE 1

SmartCard Types : Table				
SmartCard Type	Type	Manufacturer	Version	Number
12	LDAPBind	Bind to an LDAP Server to authenticate a users identity	1	3
13	(AutoNumber)			0
4903	4905	4907		

4901

Proxy Definitions : Table				
Proxy ID	Name	Description	Type	Resource
1	344148459 LDAPBind	Web service proxy	1	1
AutoNumber			0	0
4911	4913	4915		4917

4902

FIG. 49

Proxy Parameter Definitions : Table				
Proxy Parameter ID	Proxy Parameter Name	Description	Value	
-1287893664	Cookie TTL	Cookie time to live in [seconds]	2580	5013
-255422959	Queries	Defined queries	Step1_Step2	5015
581256871	Step1/DLL Function	Function name in query DLL	LDAPBindAuth	5016
-1513472258	Step1/DLL Name	Query's DLL name	ClientAuth.DLL	
704661805	Step1/Include In Cookie	Include query results in cookie	1	5019
-838120726	Step1/Maximum Execution Time	Maximum query execution time in [seconds]	0	5021
922587944	Step1/Port		389	
1170892639	Step1/ProfileAttribute		Room*	
237910181	Step1/ProfileAttribute		WorkPhone*	
1513326004	Step1/ProfileAttribute		EM*	5023
994536844	Step1/Required	Query is required for authentication	1	
97150755	Step1/Saver		betelgeuse	5023
2127099161	Step1/UserDN		\$(UserID)	
-945271402	Step1/UserPwd		\$(UserPwd)	5023
1498465115	Step2/DLL Function	Function name in query DLL	GetNTUserGroups	
-1253821694	Step2/DLL Name	Query's DLL name	ClientAuth	5023
423126273	Step2/Include In Cookie	Include query results in cookie	1	
350791470	Step2/Maximum Execution Time	Maximum query execution time in [seconds]	0	5023
412661527	Step2/NTDomain		INTERDYN	
-1837754112	Step2/Required	Query is required for authentication	0	5023
437704972	Step2/UserID		\$(UserID)	
604303133	Step2/UserPwd		\$(UserPwd)	5011
5003	5005	5007	5009	5011

5001

Smartcard Definitions : Table				
Smartcard ID	Name	App ID	Code	Description
1175318406	TonyM	947715538		RoomNumber=2236*
(AutoNumber)		0		

5033

5031

5029

5027

5025

FIG. 50


Conclave Authentication Using LDAP Bind - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites History Mail

Address http://pluto.interdyn.com/BindNeptune.html

Links Internet Local Queries Alavista Bandwidth BitNet Virus

 **Authenticating Web Server**

In order to gain access to the resource you requested (BindNeptune.html &GET&192.168.36.217&pluto.interdyn.com&80&0), you are required to provide the system with the following information.

User ID: 5103

Password: 5105

5107

5101

FIG. 51

```

select Cookie, IdentityIsValid, IsAllowed, reasoncode,
       maybelist, cookiemodified
from policyeval
where sourceip='192.168.36.215' and

```

```

       application='WS' and

```

```

       resource='BindNeptune.html&GET&192.168.36.217&

```

```

       pluto.interdyn.com&80&0'

```

```

and includeeval='Y' and

```

```

includeidentitystore='Y' and

```

```

askclientforidentities='N' and

```

```

identity= 'AUTHPOSTIDENTITY IDENTITYTYPE="LDAP Bind"&

```

5204

```

ORIGINALURL="BindNeptune.html&GET&

```

```

192.168.36.217&pluto.interdyn.com&80&0"&

```

```

AUTHTYPE="LDAP Bind"&USER="fred"&PWD="agent99"&

```

5205

```

SUBMIT1="Log in"

```

5207

5209

5211

5201

FIG. 52

5303

Cookie=CONCLAVE=COOKIEIDENTITY=COOKIEIDENTITY%26AUTHTYPE%
 3D%22LDAP%20Bind%22%26IDENTTYPE%3D%22LDAP%20Bind%
 22%26ORIGINALURL%3D%22BindNeptune.html%26GET%
 26192.168.36.217%26pluto.interdyn.com%2680%260%
 22%26SUBMIT1%3D%22Log%20in%22%26USER%3D%22fred%
 22%26UserName%3D%22cn%3Dfred%2Cou%3DQA%2Cou%
 3DEngineering%2Co%3DIDI%22&EXPIRES=Thu%2C%
 2008-Jun-2000%2000:28:41%20GMT&cn=fred&
 facsimileTelephoneNumber=805-666-5563&
 initials=ddf&mail=fred@interdyn.com&objectClass=top&
 objectClass=person&objectClass=organizationalPerson&
 objectClass=inetOrgPerson&roomNumber=2217&sn=user&
 telephoneNumber=805-652-2544&uid=fred&
 NONCE=f+7KBJmHR6/XWCTmREhmnQ& 5305
 SIG=qd0ZLcPBjMiPbGlR7C7urAXad2Q; 5307
 EXPIRES=Thu, 08-Jun-2000 00:28:41 GMT;
 MAX-AGE=960424121;

IdentityIsValid = Y 5309

IsAllowed = Y 5311

ReasonCode = 116

MaybeList = 5313

CookieModified = Y

5301

FIG. 53

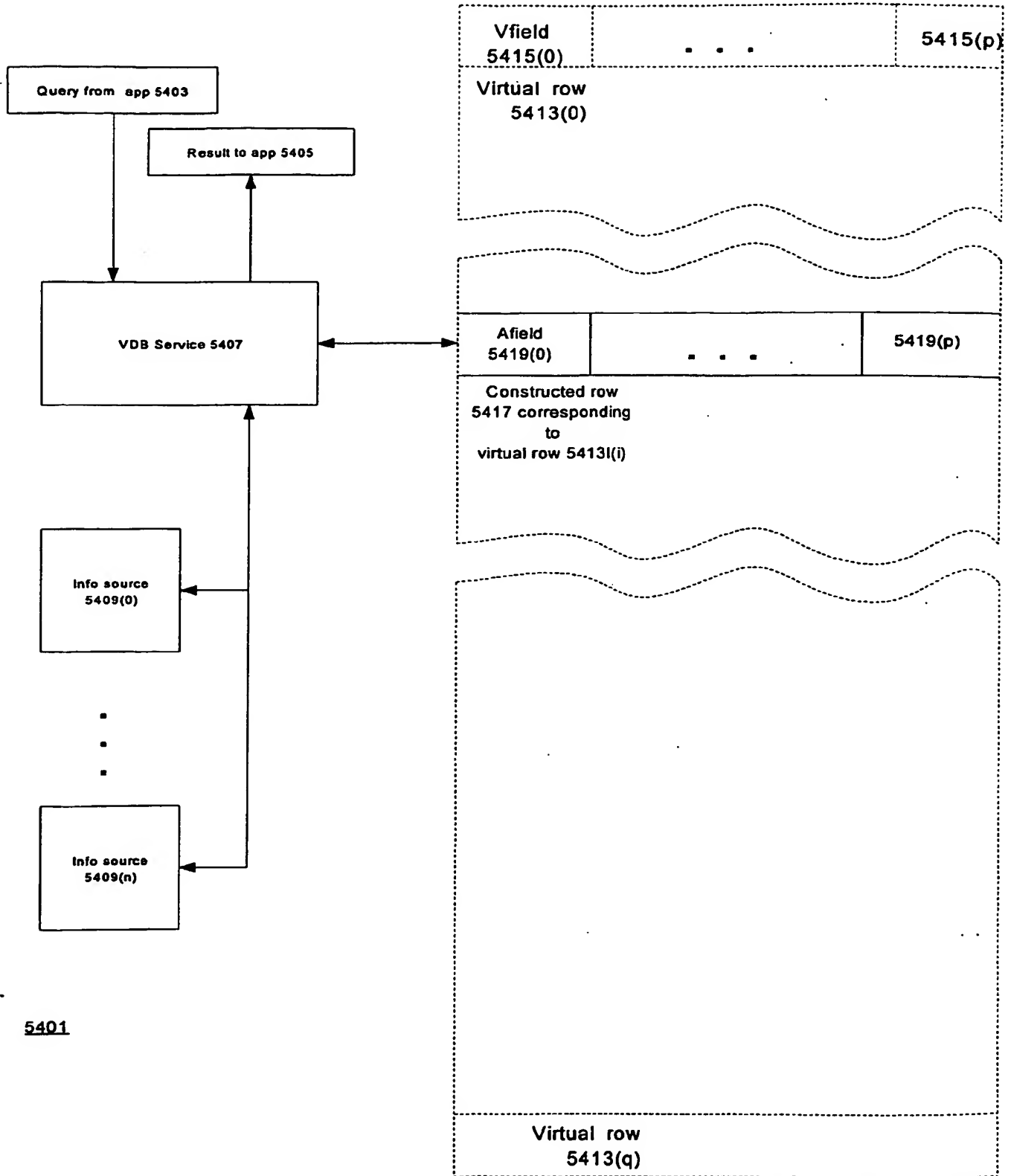


FIG. 54

Virtual relational
database table
5411